

**SIGNATURE DOCUMENT FOR
DEPARTMENT OF STATE HEALTH SERVICES
CONTRACT NO. HHS000812700042
UNDER THE
COVID-19 GRANT PROGRAM**

The parties to this agreement (“Grant Agreement” or “Contract”) are the **DEPARTMENT OF STATE HEALTH SERVICES (“SYSTEM AGENCY” OR “DSHS”)**, a pass-through entity, and **CORPUS CHRISTI-NUECES COUNTY PUBLIC HEALTH DISTRICT (CITY) (“GRANTEE”)** having its principal office at 1702 Horne Road, Corpus Christi, Texas (each a “Party” and collectively the “Parties”).

I. PURPOSE

The purpose of this Grant Agreement is to provide COVID-19 response activities.

II. LEGAL AUTHORITY

This Contract is authorized by and in compliance with the provisions of Texas Government Code Chapter 791, and Chapters 12 and 121 of the Texas Health and Safety Code.

III. DURATION

This Grant Agreement is effective on September 1, 2022 and terminates on July 31, 2024, unless renewed, extended, or terminated pursuant to the terms and conditions of the Grant Agreement.

System Agency, at its sole discretion, may extend this Grant Agreement for any period(s) of time, provided the Contract term, including all extensions or renewals, does not exceed five years. Notwithstanding the limitation in the preceding sentence, System Agency, at its sole discretion, also may extend the Contract beyond five years as necessary to ensure continuity of service, for purposes of transition, or as otherwise determined by System Agency to serve the best interest of the State.

IV. STATEMENT OF WORK

The Scope of this Grant Project to which Grantee is bound is incorporated into and made a part of this Grant Agreement for all purposes and included as **ATTACHMENT A**.

V. BUDGET

The amount of this Grant Agreement for COVID-19 epidemiologic and surveillance response (Epi) activities will be **\$855,347.00** and the amount for COVID-19 laboratory response network (LRN) activities will be **\$96,302.00**. The total amount of this Grant

Agreement will not exceed **\$951,649.00**. Grantee is not required to provide matching funds.

The total not-to-exceed amount includes the following:

Total Federal Funds: \$951,649.00
Total State Funds: \$0.00

All expenditures under the Grant Agreement will be in accordance with **ATTACHMENT B, BUDGET**.

VI. REPORTING REQUIREMENTS

This Grant Agreement contains reporting requirements as stated in **ATTACHMENT A, STATEMENT OF WORK**.

VII. CONTRACT REPRESENTATIVES

The following will act as the representative authorized to administer activities under this Contract on behalf of their respective Party.

System Agency

Department of State Health Services
P.O. Box 149347 – Mail Code 1990
Austin, Texas 78714-9347
Attention: Caeli Paradise

Grantee

Corpus Christi-Nueces County Public Health District
1702 Horne Road
Corpus Christi, Texas 78416-1902
Attention: Steven Viera

VIII. NOTICE REQUIREMENTS

- A. All notices given by Grantee shall be in writing, include the Grant Agreement contract number, comply with all terms and conditions of the Grant Agreement, and be delivered to the System Agency's Contract Representative identified above.
- B. Grantee shall send legal notices to System Agency at the address below and provide a copy to the System Agency's Contract Representative:

Health and Human Services Commission
Attn: Office of Chief Counsel
4601 W. Guadalupe, Mail Code 1100
Austin, Texas 78751

With copy to

Department of State Health Services
Attn: General Counsel
P.O. Box 149347, MC 1919
Austin, Texas 78714-9347

- C. Notices given by System Agency to Grantee may be emailed, mailed or sent by common carrier. Email notices shall be deemed delivered when sent by System Agency. Notices sent by mail shall be deemed delivered when deposited by the System Agency in the United States mail, postage paid, certified, return receipt requested. Notices sent by common carrier shall be deemed delivered when deposited by the System Agency with a common carrier, overnight, signature required.
- D. Notices given by Grantee to System Agency shall be deemed delivered when received by System Agency.
- E. Either Party may change its Contract Representative or Legal Notice contact by providing written notice to the other Party.

IX. FEDERAL AWARD INFORMATION

GRANTEE'S DATA UNIVERSAL NUMBERING SYSTEM (DUNS) NUMBER: 078495025

Federal funding under this Grant Agreement is a subaward under the following federal award.

Federal Award Identification Number (FAIN): NU50CK000501

- A. Epidemiology and Laboratory Capacity for Infectious Diseases (ELC) – 93.323-\$951,649.00
- B. Federal Award Date: April 23, 2020
- C. Federal Award Period: 8/1/2019 – 7/31/2024
- D. Name of Federal Awarding Agency: Centers for Disease Control and Prevention
- E. Federal Award Project Description: Epidemiology and Laboratory Capacity for Prevention and Control of Emerging Infectious Diseases
- F. Awarding Official Contact Information:
Brownie Anderson-Rana, Grants Management Officer
2939 Flowers Road – Mailstop TV2
Atlanta, GA 30341-5509
Phone: 770-488-2771
- G. Total Amount of Federal Funds Awarded to System Agency: \$2,068,114,803.00
- H. Amount of Funds Awarded to Grantee: \$951,649.00
- I. Identification of Whether the Award is for Research and Development: No

X. **ATTACHMENT C, UNIFORM TERMS AND CONDITIONS (VERSION 3.0) (“UTCs”)**, of this Grant Agreement is revised as follows. Unless expressly modified, amended, or replaced in this Section, the UTCs shall remain in full force and effect.

- **Section 8.5 Confidentiality**, of the UTCs, is hereby amended to add the following:

System Agency acknowledges that Grantee is a Governmental Entity and is subject to the Texas Public Information Act, and that Grantee will comply with System Agency's request for confidentiality to the extent permitted by law.

- **Section 10.1 General Indemnity**, of the UTCs, is hereby amended to add the following:

System Agency acknowledges that Grantee has been organized pursuant to the Constitution and laws of the State of Texas, possesses certain rights and privileges, is subject to certain limitations and restrictions, and only has such authority as is granted to it under the Constitution and laws of the State of Texas. No provision of this Contract extends Grantee’s liability beyond the liability or authority provided in the Constitution and the laws of the State of Texas.

To the extent permitted by the Texas Constitution, laws and rules, and without waiving any immunities or defenses available to Grantee as a governmental entity, Grantee shall be solely responsible for its own acts and omissions and the acts and omissions of its employees, directors, officers, Subcontractors and agents. System Agency shall be solely responsible for its own acts and omissions.

XI. **CONTRACT DOCUMENTS**

The following documents are incorporated by reference and made a part of this Grant Agreement for all purposes.

Unless expressly stated otherwise in this Grant Agreement, in the event of conflict, ambiguity or inconsistency between or among any documents, all System Agency documents take precedence over Grantee’s documents and the Data Use Agreement takes precedence over all other contract documents.

ATTACHMENT A - STATEMENT OF WORK

ATTACHMENT B - BUDGET

ATTACHMENT C - UNIFORM TERMS AND CONDITIONS - GRANT

ATTACHMENT D - ADDITIONAL PROVISIONS

ATTACHMENT E - FEDERAL ASSURANCES NON-CONSTRUCTION

ATTACHMENT F - CERTIFICATION REGARDING LOBBYING

ATTACHMENT G - FFATA

ATTACHMENT H - HHS DATA USE AGREEMENT
ATTACHMENT I - SECURITY AND PRIVACY INQUIRY (SPI)

XII. SIGNATURE AUTHORITY

Each Party represents and warrants that the person executing this Grant Agreement on its behalf has full power and authority to enter into this Grant Agreement. Any services or work performed by Grantee before this Grant Agreement is effective or after it ceases to be effective are performed at the sole risk of Grantee.

SIGNATURE PAGE FOLLOWS

**SIGNATURE PAGE FOR SYSTEM AGENCY
CONTRACT NO. HHS000812700042**

SYSTEM AGENCY

DocuSigned by:
Imelda Garcia
87AFD32AD9D24A9...

Signature

Printed Name: Imelda Garcia

Title: Associate Commissioner

Date of Execution: June 13, 2022

GRANTEE

DocuSigned by:
Steven Viera
7A188293F923439...

Signature

Printed Name: Steven Viera

Title: Interim Director of Health

Date of Execution: May 16, 2022

**ATTACHMENT A
STATEMENT OF WORK**

I. GRANTEE RESPONSIBILITIES

Grantee will:

A. Enhance public health follow-up activities, including:

1. Conducting case investigations;
2. Eliciting or identifying individuals who may have been exposed to COVID-19;
3. Notifying individuals of COVID-19 exposure; and
4. Providing referrals to COVID-19 testing, vaccine resources and other follow-up services.

Data must be entered into the DSHS data system in accordance with DSHS published guidance. Grantee may not incur COVID-19 contact tracing Call Center expenditures beyond 8/31/2021.

B. Improve morbidity and mortality surveillance, including:

1. Establish or enhance community-based surveillance - Surveillance of populations and individuals includes but is not limited to those without severe illness, those with travel to high-risk locations, or those who are contacts to known cases.
2. Monitor and report daily COVID-19 probable and confirmed COVID cases (including deaths) to DSHS.
3. Track and send Emergency Department and outpatient visits for coronavirus (COVID)-like illness, as well as other illnesses, to Texas Syndromic Surveillance System (TxS2).
4. Send copies of all admission, discharge, and transfer (ADT) messages to the Centers for Disease Control and Prevention (CDC) National Syndromic Surveillance Program (NSSP).
5. Monitor and utilize available data in the CDC's National Healthcare Safety Network (NHSN) for confirmed 2019 novel coronavirus (COVID-19) infection or for COVID-like illness.
 - a. Long-term care: <https://www.cdc.gov/nhsn/ltc/covid19/index.html>
 - b. Acute care: <https://www.cdc.gov/nhsn/acute-care-hospital/covid19/index.html>
6. Work with long-term care facilities to enroll the facility in the NHSN Long-Term Care Facility (LTCF) COVID-19 Module.
7. Provide requested information on COVID-19 associated deaths to DSHS within three business days.

C. Enhance laboratory testing and reporting capacity:

1. Establish or expand capacity to test all symptomatic individuals, and secondarily expand capacity to achieve community-based surveillance. This capacity would entail increasing testing capabilities above the current number of specimens that can be tested at the jurisdiction's public health laboratory or by establishing new testing capabilities at the jurisdiction's laboratory.
2. Screen for past infection (e.g., serology) for health care workers, employees of high-risk facilities, critical infrastructure workforce, and childcare providers.
3. Obtain all jurisdictional laboratory test data electronically, including from new, non-traditional testing settings, and using alternative file formats (e.g., .csv or .xls) to help automate. In addition to other reportable results, this should include all COVID-19-related testing data, including all tests to detect severe acute respiratory syndrome coronavirus 2 (SAR-CoV-2) and serology testing.
4. Report all COVID-19-related line level testing data (negatives, positives, indeterminates, serology) daily to DSHS. Data must meet new federal Coronavirus Aid, Relief, and Economic Security (CARES) Act laboratory guidance. All public health data must be reported electronically to DSHS in compliance with the Texas Administrative Code and within appropriate reporting timeframes.

D. Prevent and control COVID-19 in healthcare settings and protect other vulnerable or high-risk populations:

1. Assess and monitor COVID-19 infections in healthcare workers across the healthcare spectrum.
2. Perform infection control assessments using preparedness tools approved by DSHS to ensure interventions are in place to protect high-risk populations.
3. Monitor and help implement mitigation strategies for COVID-19 in all high-risk healthcare facilities (e.g., hospitals, dialysis clinics, cancer clinics, nursing homes, and other long-term care facilities).
4. Monitor and help implement mitigation strategies for other high-risk employment settings (e.g., meat processing facilities) and congregate living settings (e.g., prisons, youth homes, shelters).
 - a. This includes coordinating with the Texas Department of Criminal Justice when individuals are released from serving their prison term and will be returning to the jurisdiction. These individuals may have been exposed to COVID-19 while in prison and/or may be COVID-19-positive and require additional public health follow-up.

E. Monitor and mitigate COVID-19 introductions from connected jurisdictions (i.e., neighboring cities and states, including air travel).

F. Work with healthcare system to manage and monitor system capacity.

1. Assess and monitor the number and availability of critical care staff, necessary PPE and potentially life-saving medical equipment, as well as access to testing services.
 2. Leverage NHSN data to **monitor** healthcare worker staffing, Patient Impact, Hospital Capacity, and healthcare supplies (PPE, PAPRs, ventilators, etc.). Grantee will request access to the NHSN database within 30 days of the execution of this Contract or within 30 days of hire for the position completing the data entry. Upon access approval, Grantee will review available NHSN data (at least monthly) to assess gaps in the healthcare system.
- G. Improve understanding of jurisdictional communities with respect to COVID-19 risk. Grantee must build an understanding of population density and high-risk population density (i.e., population of >65 yrs., proportion of population with underlying conditions, households with limited English fluency, healthcare-seeking behavior, populations without insurance and those below poverty level).
- H. Submit a quarterly report on the report template to be provided by DSHS. Quarterly reports are due on or before the 15th of the month following the end of the quarter being reported on. Each report must contain a summary of activities that occurred during the preceding quarter for each activity listed above in Section I, A through G. Submit quarterly reports by electronic mail to COVID.Contracts@dshs.texas.gov. The email "Subject Line" and the name of the attached file for all reports should be clearly identified with the Grantee's Name, Contract Number, IDCU/COVID and the quarter the report covers.
- I. May use funds to pay pre-award costs which date back to January 20, 2020, that are directly related to the COVID-19 outbreak response. All pre-award costs must be approved in writing by DSHS.
- J. Not use funds for research, clinical care, fundraising activities, construction or major renovations, to supplant existing state or federal funds for activities, or funding an award to another party or provider who is ineligible. Other than normal and recognized executive-legislative relationships, no funds may be used for:
1. Publicity or propaganda purposes, for the preparation, distribution, or use of any material designed to support or defeat the enactment of legislation before any legislative body;
 2. The salary or expenses of any grant or contract recipient, or agent acting for such recipient, related to any activity designed to influence the enactment of legislation, appropriations, regulation, administrative act or Executive order proposed or pending before any legislative body.
- K. Controlled Assets include firearms, regardless of the acquisition cost, and the following assets with an acquisition cost of \$500 or more, but less than \$5,000:

desktop and laptop computers (including notebooks, tablets and similar devices), non-portable printers and copiers, emergency management equipment, communication devices and systems, medical and laboratory equipment, and media equipment. Controlled Assets are considered Supplies.

L. Grantee shall maintain an inventory of Equipment, supplies defined as Controlled Assets, and real property and submit an annual cumulative report of the equipment and other property on the DSHS Contractor's Property Inventory Report located at <https://www.dshs.texas.gov/hivstd/contractor/cmsforms.shtm> to CMSInvoices@dshs.texas.gov and COVID.Contracts@dshs.texas.gov not later than October 15 of each year. If Grantee did not purchase Equipment or other property, this report is still required to be submitted.

M. DSHS funds must not be used to purchase buildings or real property without prior written approval from DSHS. Any costs related to the initial acquisition of the buildings or real property are not allowable without written pre-approval.

N. At the expiration or termination of this Contract for any reason, title to any remaining equipment and supplies purchased with funds under this Contract reverts to DSHS. Title may be transferred to any other party designated by DSHS. DSHS may, at its option and to the extent allowed by law, transfer the reversionary interest to such property to Grantee.

II. PERFORMANCE MEASURES

The System Agency will monitor the Grantee's performance of the requirements in Attachments A and A-1 and compliance with the Contract's terms and conditions.

III. INVOICE AND PAYMENT

A. Grantee will request payments using the State of Texas Purchase Voucher (Form B-13) located at <https://www.dshs.texas.gov/hivstd/contractor/cmsforms.shtm>. Voucher and any supporting documentation will be mailed or submitted by fax or electronic mail to all addresses/number below.

Department of State Health Services
Claims Processing Unit, MC 1940
1100 West 49th Street
P.O. Box 149347
Austin, TX 78714-9347
FAX: (512) 458-7442
EMAIL: invoices@dshs.state.tx.us and
EMAIL: CMSInvoices@dshs.texas.gov and
EMAIL: COVID.Contracts@dshs.texas.gov

- B.** Grantee will be paid on a cost reimbursement basis and in accordance with the Budget in Attachment B of this Contract.
- C.** Grantee will submit requests for reimbursement (Form B-13) and financial expenditure template monthly by the last business day of the month following the month in which expenses were incurred or services provided. Grantee shall maintain all documentation that substantiates invoices and make the documentation available to DSHS upon request. In the event a cost reimbursed under the Contract is later determined to be unallowable, then the Grantee will reimburse DSHS for that cost.
- D.** Grantee will submit quarterly Financial Status Reports (FSRs) to DSHS by the last business day of the month following the end of each quarter of the Contract for DSHS review and financial assessment.
- E.** Grantee will submit request for reimbursement (B-13) as a final close-out invoice not later than forty-five (45) calendar days following the end of the term of the Contract. Reimbursement requests received in the DSHS office more than forty-five (45) calendar days following the termination of the Contract may not be paid.
- F.** Grantee will submit a final FSR as a final close-out FSR not later than forty-five (45) calendar days following the end of the term of the Contract.

**ATTACHMENT A-1
SUPPLEMENTAL STATEMENT OF WORK**

IV. GRANTEE RESPONSIBILITIES

Grantee will perform activities as submitted in their DSHS approved budgets for this specific funding Contract period. All activities must be listed below to be approved for this funding and any additional activities not listed in the approved budget must be submitted for DSHS consideration and approval. The activities for this Contract funding period are as follows:

A. Enhance Laboratory, Surveillance, Informatics and other Workforce Capacity, including:

1. Train and hire staff to improve laboratory workforce ability to address issues around laboratory safety, quality management, inventory management, specimen management, diagnostic and surveillance testing and reporting results.
2. Build expertise for healthcare and community outbreak response and infection prevention and control (IPC) among local health departments.
3. Train and hire staff to improve the capacities of the epidemiology and informatics workforce to effectively conduct surveillance and response of COVID-19 (including case investigation and public health follow-up activities) and other emerging infections and conditions of public health significance. This should include staff who can address unique cultural needs of those at higher risk for COVID-19. Grantee may not incur COVID-19 contact tracing or contact tracing call center expenditures after 08/31/2021.
4. Build expertise to support management of the COVID-19-related activities within the jurisdiction and integrate into the broader Epidemiology and Laboratory Capacity (ELC) portfolio of activities (e.g., additional leadership, program and project managers, budget staff, etc.).
5. Increase capacity for timely data management, analysis, and reporting for COVID-19 and other emerging coronavirus and other infections and conditions of public health significance.

B. Strengthen Laboratory Testing

1. Establish or expand capacity to quickly, accurately and safely test for SARS-CoV-2/COVID-19 and build infectious disease preparedness for future coronavirus and other events involving other pathogens with potential for broad community spread.

- a. Develop systems to improve speed and efficiency of specimen submission to clinical and reference laboratories.
 - b. Strengthen ability to rapidly respond to testing (e.g., nucleic acid amplification test [NAAT], antigen, etc.) as necessary to ensure that optimal utilization of existing and new testing platforms can be supported to help meet increases in testing demand in a timely manner. Laboratory Response Networks (LRNs) and Local Health Departments (LHDs) with laboratories are strongly encouraged to diversify their testing platforms to enable them to pivot depending on reagent and supply availabilities.
 - c. Perform serology testing with an FDA Emergency Use Authorization (EUA) authorized serological assay as appropriate to respond to emerging pandemics in order to conduct surveillance for past infection and monitor community exposure.
 - d. Build local capacity for testing of COVID-19/SARS-CoV-2 including within high-risk settings or in vulnerable populations that reside in their communities.
 - e. Apply laboratory safety methods to ensure worker safety when managing and testing samples that may contain SARS-CoV-2/COVID-19.
 - f. Laboratories and LRNs are encouraged to implement new technologies to meet local needs.
 - g. Augment or add specificity to existing laboratory response plans for future coronavirus and other outbreak responses caused by an infectious disease. Provider must be able to establish a plan to maintain the activity when the funds are no longer available. This is an optional activity.
2. Enhance laboratory testing capacity for SARS-CoV-2/COVID-19 by ensuring public/private laboratory testing providers have access to biosafety resources for SARS-CoV-2 specimen collection and/or testing.

C. Advance Electronic Data Exchange at Public Health Labs

1. Enhance and expand laboratory information infrastructure, to improve jurisdictional visibility on laboratory data (tests performed) from all testing sites and enable faster and more complete data exchange and reporting with DSHS.
 - a. Employ a well-functioning Laboratory Information Management System (LIMS) to support efficient data flows within the PHL and its partners. This includes expanding existing capacity of the current LIMS to improve data exchange and increase data flows through LIMS maintenance, new configurations/modules, and enhancements. Implement new/replacement LIMS where needed.

Note: If implementing new or replacement systems, develop an implementation plan, including appropriate milestones and timeline to completion. Implementation plans will be reviewed and approved for consistency with the activities set forth by DSHS prior to start of

implementation. Completion of the implementation plan is DSHS verifying that the submitted electronic laboratory reporting (ELR) feeds have been successfully processed in National Electronic Disease Surveillance System (NEDSS).

- b. Ensure ability to administer LIMS. Ensure the ability to configure all tests that are in LIMS, including new tests, EUAs, etc., in a timely manner. Ensure expanding needs for administration and management of LIMS are covered through dedicated staff.
- c. Interface diagnostic equipment to directly report laboratory results into LIMS.

D. Improve Surveillance and Reporting of Electronic Health Data

1. Establish complete, up-to-date, timely reporting of morbidity and mortality to DSHS due to COVID-19 and other coronavirus and other emerging infections which impact conditions of public health significance, with required associated data fields in a machine-readable format, by:
 - a. Establishing or enhancing community-based surveillance, including surveillance of vulnerable populations, individuals without severe illness, those with recent travel to high-risk locations, or who are contacts to known cases.
 - b. Monitoring changes to daily incidence rates of COVID-19 and other conditions of public health significance at the county or Zip code level to inform community mitigation strategies.
2. Establish additional and ongoing surveillance methods (e.g., sentinel surveillance) for COVID-19 and other conditions of public health significance.
3. At the health department, enhance capacity to work with testing facilities to onboard and improve ELR, including to receive data from new or non-traditional testing settings. Use alternative data flows (e.g., reporting portals) and file formats (e.g., CSV or XLS) to help automate where appropriate. In addition to other reportable results, this should include all COVID-19/SARS-CoV-2-related testing data (i.e., tests to detect SARS-CoV-2 including serology testing).
4. Improve understanding of capacity, resources, and patient impact at healthcare facilities through electronic reporting.
 - a. Require expansion of reporting facility capacity, resources, and patient impact information, such as patients admitted and hospitalized, in an electronic, machine-readable, as well as human-readable, visual and tabular manner, to achieve 100% coverage in jurisdiction and include daily data from all acute care, long-term care, and ambulatory care

- settings. Use these data to monitor facilities with confirmed cases of COVID-19/SARS-CoV-2 infection or with COVID-like illness among staff or residents and facilities at high risk of acquiring COVID-19/SARS-CoV-2 cases and COVID-like illness among staff or residents.
- b. Increase Admit, Discharge, Transfer (ADT) messaging and use to achieve comprehensive surveillance of emergency room visits, hospital admissions, facility and department transfers, and discharges to provide an early warning signal, to monitor the impact on hospitals, and to understand the growth of serious cases requiring admission.
5. Establish or improve systems to ensure complete, accurate and immediate (within 24 hours) data transmission that allows for automated transmission of data to DSHS in a machine-readable format.

Note: Use of an existing DSHS system is preferred. If implementing new or replacement systems, develop an implementation plan, including the process for automatic transmission of data to DSHS in a machine-readable format, appropriate milestones and timeline to completion. Implementation plans will be reviewed and approved for consistency with the activities set forth by DSHS prior to start of implementation.

 - a. Submit all case reports in an immediate way to DSHS for COVID-19/SARS-CoV-2 and other conditions of public health significance with associated required data fields in a machine-readable format.
 - b. Report requested COVID-19/SARS-CoV-2-related data, including line level testing data (negatives, positives, indeterminates, serology, antigen, nucleic acid) daily by county or Zip code to DSHS.
 - c. Establish these systems in such a manner that they may be used on an ongoing basis for surveillance of, and reporting on, routine and other threats to the public health and conditions of public health significance.

E. Use Laboratory Data to Enhance Investigation, Response and Prevention

1. Use laboratory data to initiate and conduct case investigation and public health follow-up activities and implement containment measures.
 - a. Conduct necessary case investigation and public health follow-up activities including contact elicitation/identification, contact notification, contact testing, and follow-up. Activities could include traditional case investigation and public health follow-up activities and/or proximity/location-based methods, as well as methods adapted for healthcare facilities, employers, elementary and secondary schools, childcare facilities, institutions of higher education or in other settings. Data must be entered into the DSHS data system in accordance with DSHS published guidance. Grantee may not incur COVID-19 contact tracing call center expenditures beyond 8/31/2021.

- b. Utilize tools (e.g., geographic information systems and methods) that assist in the rapid mapping and tracking of disease cases for timely and effective epidemic monitoring and response, incorporating laboratory testing results and other data sources.
 - c. Assist in identifying facilities that are not submitting data through ELR. Provide these facilities with information on the ELR onboarding process and the appropriate contact information of DSHS team who can onboard the facility to have their data be reported electronically and no longer sent by fax. Also provide the names of these facilities to the DSHS team.
 2. Identify cases and exposure to COVID-19 in high-risk settings or within populations at increased risk of severe illness or death to target mitigation strategies and referral for therapies (for example, monoclonal antibodies) to prevent hospitalization.
 - a. Assess and monitor infections in healthcare workers across the healthcare spectrum.
 - b. Monitor cases and exposure to COVID-19 to identify need for targeted mitigation strategies to isolate and prevent further spread within high-risk healthcare facilities (e.g., hospitals, dialysis clinics, cancer clinics, nursing homes, other long-term care facilities, etc.).
 - c. Monitor cases and exposure to COVID-19 to identify need for targeted mitigation strategies to isolate and prevent further spread within high-risk occupational settings (e.g., meat processing facilities) and congregate living settings (e.g., correctional facilities, youth homes, shelters).
 - d. Work with DSHS to build capacity for reporting, rapid containment and prevention of COVID-19/SARS-CoV-2 within high-risk settings or in vulnerable populations that reside in their communities.
 - e. Jurisdictions should ensure systems are in place to link test results to relevant public health strategies, including prevention and treatment.

Note: Utilization of an existing DSHS system is preferred. If implementing new or replacement systems, develop an implementation plan, including the process for automatic transmission of data to DSHS in a machine-readable format, appropriate milestones and timeline to completion. Implementation plans will be reviewed and approved for consistency with the activities set forth by DSHS prior to start of implementation.
3. Implement prevention strategies in high-risk settings or within vulnerable populations (including tribal nations as appropriate), including proactive monitoring for asymptomatic case detection.

Note: These additional resources are intended to be directed toward testing, case investigation and public health follow-up activities, surveillance, containment, and mitigation, including support for workforce, epidemiology, use by employers, elementary and secondary schools,

childcare facilities, institutions of higher education, long-term care facilities, or in other settings, scale-up of testing by public health, academic, commercial, and hospital laboratories, and community-based testing sites, mobile testing units, healthcare facilities, and other entities engaged in COVID–19 testing, and other related activities related to COVID–19 testing, case investigation and public health follow-up activities, surveillance, containment, and mitigation which may include interstate compacts or other mutual aid agreements for such purposes.

- a. Build capacity for infection prevention and control in long-term care facilities (LTCFs) (e.g., at least one Infection Preventionist [IP] for every facility) and outpatient settings.
 - i. Build capacity for LTCFs to safely care for infected and exposed residents of LTCFs and other congregate settings.
 - ii. Assist with enrollment of all LTCFs into CDC’s National Healthcare Safety Network NHSN at <https://www.cdc.gov/nhsn/ltc/enroll.html>.
 - b. Build capacity for infection prevention and control in elementary and secondary schools, childcare facilities, and/or institutions of higher education.
 - c. Increase Infection Prevention and Control (IPC) assessment capacity on site using tele-ICAR.
 - d. Perform preparedness assessment to ensure interventions are in place to protect high-risk populations.
 - e. Coordinate as appropriate with federally funded entities responsible for providing health services to higher-risk populations (e.g., tribal nations and federally qualified health centers).
- F.** Submit a quarterly report on the report template to be provided by DSHS. Quarterly reports are due on or before the 15th of the month following the end of the quarter. Each report must contain a summary of activities that occurred during the preceding quarter for each activity listed above in Section I, Subsections A through E. Submit quarterly reports by electronic mail to COVID.Contracts@dshs.texas.gov. The email “Subject Line” and the name of the attached file for all reports should be clearly identified with the Grantee’s Name, Contract Number, IDCU/COVID and the quarter the report covers.
- G.** Not use funds for research, clinical care, fundraising activities, construction or major renovations, to supplant existing state or federal funds for activities, or funding an award to another party or provider who is ineligible. Other than normal and recognized executive-legislative relationships, no funds may be used for:
3. Publicity or propaganda purposes, for the preparation, distribution, or use of any material designed to support or defeat the enactment of legislation before any legislative body;

4. The salary or expenses of any grant or contract recipient, or agent acting for such recipient, related to any activity designed to influence the enactment of legislation, appropriations, regulation, administrative act or Executive order proposed or pending before any legislative body.
- K. Controlled Assets include firearms, regardless of the acquisition cost, and the following assets with an acquisition cost of \$500 or more, but less than \$5,000: desktop and laptop computers (including notebooks, tablets and similar devices), non-portable printers and copiers, emergency management equipment, communication devices and systems, medical and laboratory equipment, and media equipment. Controlled Assets are considered Supplies.
- L. Grantee shall maintain an inventory of Equipment, supplies defined as Controlled Assets, and real property and submit an annual cumulative report of the equipment and other property on the DSHS Contractor's Property Inventory Report located at <https://www.dshs.texas.gov/hivstd/contractor/cmsforms.shtm> to CMSInvoices@dshs.texas.gov and COVID.Contracts@dshs.texas.gov not later than October 15 of each year. If Grantee did not purchase Equipment or other property, this report is still required to be submitted.
- M. DSHS funds must not be used to purchase buildings or real property without prior written approval from DSHS. Any costs related to the initial acquisition of the buildings or real property are not allowable without written pre-approval.
- N. At the expiration or termination of this Contract for any reason, title to any remaining equipment and supplies purchased with funds under this Contract reverts to DSHS. Title may be transferred to any other party designated by DSHS. DSHS may, at its option and to the extent allowed by law, transfer the reversionary interest to such property to Grantee.

**ATTACHMENT B
BUDGET**

Categorical Budget	Epi Expansion Funding	LRN Expansion Funding	
Budget Period	Sept 1, 2022 to Aug 31, 2024	Sept 1, 2022 to Aug 31, 2024	Contract Total
PERSONNEL	\$584,568.00	\$0.00	\$584,568.00
FRINGE BENEFITS	\$243,648.00	\$0.00	\$243,648.00
TRAVEL	\$12,131.00	\$0.00	\$12,131.00
EQUIPMENT	\$0.00	\$0.00	\$0.00
SUPPLIES	\$15,000.00	\$96,302.00	\$111,302.00
CONTRACTUAL	\$0.00	\$0.00	\$0.00
OTHER	\$0.00	\$0.00	\$0.00
TOTAL DIRECT CHARGES	\$855,347.00	\$96,302.00	\$951,649.00
INDIRECT CHARGES	\$0.00	\$0.00	\$0.00
TOTAL	\$855,347.00	\$96,302.00	\$951,649.00



TEXAS

Health and Human Services

Health and Human Services (HHS)

Uniform Terms and Conditions - Grant

Version 3.0

Published and Effective – August 2021

Responsible Office: Chief Counsel

ABOUT THIS DOCUMENT

In this document, Grantees (also referred to in this document as subrecipients or contractors) will find requirements and conditions applicable to grant funds administered and passed-through by both the Texas Health and Human Services Commission (HHSC) and the Department of State Health Services (DSHS). These requirements and conditions are incorporated into the Grant Agreement through acceptance by Grantee of any funding award by HHSC or DSHS.

The terms and conditions in this document are in addition to all requirements listed in the RFA, if any, under which applications for this grant award are accepted, as well as all applicable federal and state laws and regulations. Applicable federal and state laws and regulations may include, but are not limited to: 2 CFR Part 200, Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards; requirements of the entity that awarded the funds to HHS; Chapter 783 of the Texas Government Code; Texas Comptroller of Public Accounts' agency rules (including Uniform Grant and Contract Standards set forth in Title 34, Part 1, Chapter 20, Subchapter E, Division 4 of the Texas Administrative Code); the Texas Grant Management Standards (TxGMS) developed by the Texas Comptroller of Public Accounts; and the Funding Announcement, Solicitation, or other instrument/documentation under which HHS was awarded funds. HHS, in its sole discretion, reserves the right to add requirements, terms, or conditions.

TABLE OF CONTENTS

ARTICLE I. DEFINITIONS AND INTERPRETIVE PROVISIONS	6
1.1 DEFINITIONS	6
1.2 INTERPRETIVE PROVISIONS.....	7
ARTICLE II. PAYMENT PROVISIONS	8
2.1 PROMPT PAYMENT.....	8
2.2 TAXES	8
2.3 ANCILLARY AND TRAVEL EXPENSES	9
2.4 BILLING.....	9
2.5 USE OF FUNDS	9
2.6 USE FOR MATCH PROHIBITED.....	9
2.7 PROGRAM INCOME	9
2.8 NONSUPPLANTING.....	9
2.9 INDIRECT COST RATES.....	10
ARTICLE III. STATE AND FEDERAL FUNDING	10
3.1 EXCESS OBLIGATIONS PROHIBITED.....	10
3.2 NO DEBT AGAINST THE STATE.....	10
3.3 DEBTS AND DELINQUENCIES	10
3.4 REFUNDS AND OVERPAYMENTS	10
ARTICLE IV. ALLOWABLE COSTS AND AUDIT REQUIREMENTS	11
4.1 ALLOWABLE COSTS	11
4.2 AUDITS AND FINANCIAL STATEMENTS.....	11
4.3 SUBMISSION OF AUDITS AND FINANCIAL STATEMENTS	12
ARTICLE V. WARRANTY, AFFIRMATIONS, ASSURANCES AND CERTIFICATIONS.....	12
5.1 WARRANTY	12
5.2 GENERAL AFFIRMATIONS.....	13
5.3 FEDERAL ASSURANCES	13
5.4 FEDERAL CERTIFICATIONS	13
5.5 STATE ASSURANCES.....	13

ARTICLE VI. INTELLECTUAL PROPERTY	13
6.1 OWNERSHIP OF WORK PRODUCT.....	13
6.2 GRANTEE’S PRE-EXISTING WORKS	14
6.3 THIRD PARTY IP	14
6.4 AGREEMENTS WITH EMPLOYEES AND SUBCONTRACTORS	14
6.5 DELIVERY UPON TERMINATION OR EXPIRATION	14
6.6 SURVIVAL	15
6.7 SYSTEM AGENCY DATA	15
ARTICLE VII. PROPERTY	15
7.1 USE OF STATE PROPERTY.....	15
7.2 DAMAGE TO STATE PROPERTY	16
7.3 PROPERTY RIGHTS UPON TERMINATION OR EXPIRATION OF CONTRACT	16
7.4 EQUIPMENT AND PROPERTY.....	16
ARTICLE VIII. RECORD RETENTION, AUDIT, AND CONFIDENTIALITY.....	17
8.1 RECORD MAINTENANCE AND RETENTION.....	17
8.2 AGENCY’S RIGHT TO AUDIT.....	17
8.3 RESPONSE/COMPLIANCE WITH AUDIT OR INSPECTION FINDINGS	18
8.4 STATE AUDITOR’S RIGHT TO AUDIT	18
8.5 CONFIDENTIALITY	18
ARTICLE IX. GRANT REMEDIES, TERMINATION AND PROHIBITED ACTIVITIES.....	18
9.1 REMEDIES.....	18
9.2 TERMINATION FOR CONVENIENCE	19
9.3 TERMINATION FOR CAUSE	19
9.4 GRANTEE RESPONSIBILITY FOR SYSTEM AGENCY’S TERMINATION COSTS....	20
9.5 INHERENTLY RELIGIOUS ACTIVITIES	20
9.6 POLITICAL ACTIVITIES.....	20
ARTICLE X. INDEMNITY.....	21
10.1 GENERAL INDEMNITY.....	21
10.2 INTELLECTUAL PROPERTY	21
10.3 ADDITIONAL INDEMNITY PROVISIONS.....	21
ARTICLE XI. GENERAL PROVISIONS	22
11.1 AMENDMENTS	22
11.2 NO QUANTITY GUARANTEES.....	22

11.3	CHILD ABUSE REPORTING REQUIREMENTS	22
11.4	CERTIFICATION OF MEETING OR EXCEEDING TOBACCO-FREE WORKPLACE POLICY MINIMUM STANDARDS	22
11.5	INSURANCE AND BONDS	23
11.6	LIMITATION ON AUTHORITY	23
11.7	CHANGE IN LAWS AND COMPLIANCE WITH LAWS	24
11.8	SUBCONTRACTORS	24
11.9	PERMITTING AND LICENSURE	24
11.10	INDEPENDENT CONTRACTOR	24
11.11	GOVERNING LAW AND VENUE	25
11.12	SEVERABILITY	25
11.13	SURVIVABILITY	25
11.14	FORCE MAJEURE	25
11.15	NO IMPLIED WAIVER OF PROVISIONS	25
11.16	FUNDING DISCLAIMERS AND LABELING	25
11.17	MEDIA RELEASES	26
11.18	PROHIBITION ON NON-COMPETE RESTRICTIONS	26
11.19	SOVEREIGN IMMUNITY	26
11.20	ENTIRE CONTRACT AND MODIFICATION	27
11.21	COUNTERPARTS	27
11.22	PROPER AUTHORITY	27
11.23	E-VERIFY PROGRAM	27
11.24	CIVIL RIGHTS	27
11.25	ENTERPRISE INFORMATION MANAGEMENT STANDARDS	28
11.26	DISCLOSURE OF LITIGATION	28
11.27	NO THIRD PARTY BENEFICIARIES	29
11.28	BINDING EFFECT	29

ARTICLE I. DEFINITIONS AND INTERPRETIVE PROVISIONS

1.1 DEFINITIONS

As used in this Grant Agreement, unless a different definition is specified, or the context clearly indicates otherwise, the following terms and conditions have the meanings assigned below:

“[Amendment](#)” means a written agreement, signed by the Parties, which documents changes to the Grant Agreement.

“[Contract](#)” or “[Grant Agreement](#)” means the agreement entered into by the Parties, including the Signature Document, these Uniform Terms and Conditions, along with any attachments and amendments that may be issued by the System Agency.

“[Deliverables](#)” means the goods, services, and work product, including all reports and project documentation, required to be provided by Grantee to the System Agency.

“[DSHS](#)” means the Department of State Health Services.

“[Effective Date](#)” means the date on which the Grant Agreement takes effect.

“[Federal Fiscal Year](#)” means the period beginning October 1 and ending September 30 each year, which is the annual accounting period for the United States government.

“[GAAP](#)” means Generally Accepted Accounting Principles.

“[GASB](#)” means the Governmental Accounting Standards Board.

“[Grantee](#)” means the Party receiving funds under this Grant Agreement. May also be referred to as “subrecipient” or “contractor” in this document.

“[HHSC](#)” means the Texas Health and Human Services Commission.

“[Health and Human Services](#)” or “[HHS](#)” includes HHSC and DSHS.

“[Intellectual Property Rights](#)” means the worldwide proprietary rights or interests, including patent, copyright, trade secret, and trademark rights, as such right may be evidenced by or embodied in:

- i. any idea, design, concept, personality right, method, process, technique, apparatus, invention, discovery, or improvement;
- ii. any work of authorship, including any compilation, computer code, website or web page design, literary work, pictorial work, or graphic work;
- iii. any trademark, service mark, trade dress, trade name, branding, or other indicia of source or origin;
- iv. domain name registrations; and
- v. any other proprietary or similar rights. The Intellectual Property Rights of a Party include all worldwide proprietary rights or interests that the Party may have acquired by assignment, by exclusive license, or by license with the right to grant sublicenses.

“[Parties](#)” means the System Agency and Grantee, collectively.

“[Party](#)” means either the System Agency or Grantee, individually.

“[Project](#)” means specific activities of the Grantee that are supported by funds provided under this Grant Agreement.

“[Signature Document](#)” means the document executed by all Parties for this Grant Agreement.

“[Solicitation](#),” “[Funding Announcement](#)” or “[Request for Applications \(RFA\)](#)” means the document (including all exhibits, attachments, and published addenda), issued by the System Agency under which applications for grant funds were requested, which is incorporated by reference in the Grant Agreement for all purposes in its entirety.

“[Solicitation Response](#)” or “[Application](#)” means Grantee’s full and complete Solicitation response (including any attachments and addenda), which is incorporated by reference in the Grant Agreement for all purposes in its entirety.

“[State Fiscal Year](#)” means the period beginning September 1 and ending August 31 each year, which is the annual accounting period for the State of Texas.

“[State of Texas Textravel](#)” means the Texas Comptroller of Public Accounts’ state travel rules, policies, and guidelines.

“[Statement of Work](#)” means the description of activities Grantee must perform to complete the Project, as specified in the Grant Agreement and as may be amended.

“[System Agency](#)” means HHSC or DSHS, as applicable.

“[Work Product](#)” means any and all works, including work papers, notes, materials, approaches, designs, specifications, systems, innovations, improvements, inventions, software, programs, source code, documentation, training materials, audio or audiovisual recordings, methodologies, concepts, studies, reports, whether finished or unfinished, and whether or not included in the deliverables, that are developed, produced, generated or provided by Grantee in connection with Grantee’s performance of its duties under the Grant Agreement or through use of any funding provided under this Grant Agreement.

“[Texas Grant Management Standards](#)” or “[TxGMS](#)” means uniform grant and contract administration procedures, developed under the authority of Chapter 783 of the Texas Government Code, to promote the efficient use of public funds in local government and in programs requiring cooperation among local, state, and federal agencies. Under this Grant Agreement, TxGMS applies to Grantee except as otherwise provided by applicable law or directed by System Agency. Additionally, except as otherwise provided by applicable law, in the event of a conflict between TxGMS and applicable federal or state law, federal law prevails over state law and state law prevails over TxGMS.

1.2 INTERPRETIVE PROVISIONS

- A. The meanings of defined terms include the singular and plural forms.
- B. The words “hereof,” “herein,” “hereunder,” and similar words refer to this Grant Agreement as a whole and not to any particular provision, section, attachment, or schedule of this Grant Agreement unless otherwise specified.
- C. The term “including” is not limiting and means “including without limitation” and, unless otherwise expressly provided in this Grant Agreement, (i) references to contracts

(including this Grant Agreement) and other contractual instruments shall be deemed to include all subsequent Amendments and other modifications, but only to the extent that such Amendments and other modifications are not prohibited by the terms of this Grant Agreement, and (ii) references to any statute or regulation are to be construed as including all statutory and regulatory provisions consolidating, amending, replacing, supplementing, or interpreting the statute or regulation.

- D. Any references to agreements, contracts, statutes, or administrative rules or regulations in the Grant Agreement are references to these documents as amended, modified, or supplemented during the term of the Grant Agreement.
- E. The captions and headings of this Grant Agreement are for convenience of reference only and do not affect the interpretation of this Grant Agreement.
- F. All attachments, including those incorporated by reference, and any Amendments are considered part of the terms of this Grant Agreement.
- G. This Grant Agreement may use several different limitations, regulations, or policies to regulate the same or similar matters. All such limitations, regulations, and policies are cumulative.
- H. Unless otherwise expressly provided, reference to any action of the System Agency or by the System Agency by way of consent, approval, or waiver will be deemed modified by the phrase “in its sole discretion.”
- I. Time is of the essence in this Grant Agreement.
- J. Prior to execution of the Grant Agreement, Grantee must notify System Agency’s designated contact in writing of any ambiguity, conflict, discrepancy, omission, or other error. If Grantee fails to notify the System Agency designated contact of any ambiguity, conflict, discrepancy, omission or other error in the Grant Agreement prior to Grantee’s execution of the Grant Agreement, Grantee:
 - i. Shall have waived any claim of error or ambiguity in the Grant Agreement; and
 - ii. Shall not contest the interpretation by the System Agency of such provision(s).

No grantee will be entitled to additional reimbursement, relief, or time by reason of any ambiguity, conflict, discrepancy, exclusionary specification, omission, or other error or its later correction.

ARTICLE II. PAYMENT PROVISIONS

2.1 PROMPT PAYMENT

Payment shall be made in accordance with Chapter 2251 of the Texas Government Code, commonly known as the Texas Prompt Payment Act. Chapter 2251 of the Texas Government Code shall govern remittance of payment and remedies for late payment and non-payment.

2.2 TAXES

Grantee represents and warrants that it shall pay all taxes or similar amounts resulting from the Grant Agreement, including, but not limited to, any federal, State, or local income, sales or excise taxes of Grantee or its employees. System Agency shall not be liable for any taxes resulting from the Grant Agreement.

2.3 ANCILLARY AND TRAVEL EXPENSES

- A. Except as otherwise provided in the Grant Agreement, no ancillary expenses incurred by the Grantee in connection with its provision of the services or deliverables will be reimbursed by the System Agency. Ancillary expenses include, but are not limited to, costs associated with transportation, delivery, and insurance for each deliverable.
- B. Except as otherwise provided in the Grant Agreement, when the reimbursement of travel expenses is authorized by the Grant Agreement, all such expenses will be reimbursed in accordance with the rates set by the Texas Comptroller's *Texttravel* guidelines, which can currently be accessed at: <https://fmx.cpa.texas.gov/fmx/travel/texttravel/>.

2.4 BILLING

Unless otherwise provided in the Grant Agreement, Grantee shall bill the System Agency in accordance with the Grant Agreement. Unless otherwise specified in the Grant Agreement, Grantee shall submit requests for reimbursement or payment monthly by the last business day of the month following the month in which expenses were incurred or services provided. Grantee shall maintain all documentation that substantiates invoices and make the documentation available to the System Agency upon request.

2.5 USE OF FUNDS

Grantee shall expend funds under this Grant Agreement only for approved services and for reasonable and allowable expenses directly related to those services.

2.6 USE FOR MATCH PROHIBITED

Grantee shall not use funds provided under this Grant Agreement for matching purposes in securing other funding without the written approval of the System Agency.

2.7 PROGRAM INCOME

Program income refers to gross income directly generated by a supporting activity during the period of performance. Unless otherwise required under the Grant Agreement, Grantee shall use Program Income, as provided in TxGMS, to further the Project, and Grantee shall spend the Program Income on the Project. Grantee shall identify and report Program Income in accordance with the Grant Agreement, applicable law, and any programmatic guidance. Grantee shall expend Program Income during the Grant Agreement term, when earned, and may not carry Program Income forward to any succeeding term. Grantee shall refund Program Income to the System Agency if the Program Income is not expended in the term in which it is earned. The System Agency may base future funding levels, in part, upon Grantee's proficiency in identifying, billing, collecting, and reporting Program Income, and in using Program Income for the purposes and under the conditions specified in this Grant Agreement.

2.8 NONSUPPLANTING

Grant funds must be used to supplement existing, new or corresponding programming and related activities. Grant funds may not be used to supplant (replace) existing funds that have been appropriated, allocated, or disbursed for the same purpose. System Agency may conduct Grant monitoring or audits may be conducted to review, among other things, Grantee's compliance with this provision.

2.9 INDIRECT COST RATES

The System Agency may acknowledge an indirect cost rate for Grantees that is utilized for all applicable Grant Agreements. For subrecipients receiving federal funds, indirect cost rates will be determined in accordance with applicable law including, but not limited to, 2 CFR 200.414(f). For recipients receiving state funds, indirect costs will be determined in accordance with applicable law including, but not limited to, TxGMS. Grantees funded with blended federal and state funding will be subject to both state and federal requirements when determining indirect costs. In the event of a conflict between TxGMS and applicable federal law or regulation, the provisions of federal law or regulation will apply. Grantee will provide any necessary financial documents to determine the indirect cost rate in accordance with the Uniform Grant Guidance (UGG) and TxGMS.

ARTICLE III. STATE AND FEDERAL FUNDING

3.1 EXCESS OBLIGATIONS PROHIBITED

This Grant Agreement is subject to termination or cancellation, without penalty to System Agency, either in whole or in part, subject to the availability and actual receipt by System Agency of state or federal funds. System Agency is a state agency whose authority and appropriations are subject to actions of the Texas Legislature. If System Agency becomes subject to a legislative change, revocation of statutory authority, or lack of appropriated funds that would render either System Agency's or Grantee's delivery or performance under the Grant Agreement impossible or unnecessary, the Grant Agreement will be terminated or cancelled and be deemed null and void. In the event of a termination or cancellation under this Section, System Agency will not be liable to Grantee for any damages that are caused or associated with such termination or cancellation, and System Agency will not be required to give prior notice. Additionally, System Agency will not be liable to Grantee for any remaining unpaid funds under this Grant Agreement at time of termination.

3.2 NO DEBT AGAINST THE STATE

This Grant Agreement will not be construed as creating any debt by or on behalf of the State of Texas.

3.3 DEBTS AND DELINQUENCIES

Grantee agrees that any payments due under the Grant Agreement shall be directly applied towards eliminating any debt or delinquency it has to the State of Texas including, but not limited to, delinquent taxes, delinquent student loan payments, and delinquent child support during the entirety of the Grant Agreement term.

3.4 REFUNDS AND OVERPAYMENTS

- A. At its sole discretion, the System Agency may (i) withhold all or part of any payments to Grantee to offset overpayments, unallowable or ineligible costs made to the Grantee, or if any required financial status report(s) is not submitted by the due date(s); or (ii) require Grantee to promptly refund or credit - within thirty (30) calendar days of written notice – to System Agency any funds erroneously paid by System Agency which are not expressly authorized under the Grant Agreement.
- B. "Overpayments" as used in this Section include payments (i) made by the System

Agency that exceed the maximum allowable rates; (ii) that are not allowed under applicable laws, rules, or regulations; or (iii) that are otherwise inconsistent with this Grant Agreement, including any unapproved expenditures. Grantee understands and agrees that it shall be liable to the System Agency for any costs disallowed pursuant to financial and compliance audit(s) of funds received under this Grant Agreement. Grantee further understands and agrees that reimbursement of such disallowed costs shall be paid by Grantee from funds which were not provided or otherwise made available to Grantee under this Grant Agreement.

ARTICLE IV. ALLOWABLE COSTS AND AUDIT REQUIREMENTS

4.1 ALLOWABLE COSTS

- A. Allowable Costs are restricted to costs that are authorized under Texas Uniform Grant Management Standards (TxGMS) and applicable state and federal rules and laws. This Grant Agreement is subject to all applicable requirements of TxGMS, including the criteria for Allowable Costs. Additional federal requirements apply if this Grant Agreement is funded, in whole or in part, with federal funds.
- B. System Agency will reimburse Grantee for actual, allowable, and allocable costs incurred by Grantee in performing the Project, provided the costs are sufficiently documented. Grantee must have incurred a cost prior to claiming reimbursement and within the applicable term to be eligible for reimbursement under this Grant Agreement. At its sole discretion, the System Agency will determine whether costs submitted by Grantee are allowable and eligible for reimbursement. The System Agency may take repayment (recoup) from remaining funds available under this Grant Agreement in amounts necessary to fulfill Grantee's repayment obligations. Grantee and all payments received by Grantee under this Grant Agreement are subject to applicable cost principles, audit requirements, and administrative requirements including applicable provisions under 2 CFR 200, 48 CFR Part 31, and TxGMS.
- C. OMB Circulars will be applied with the modifications prescribed by TxGMS with effect given to whichever provision imposes the more stringent requirement in the event of a conflict.

4.2 AUDITS AND FINANCIAL STATEMENTS

- A. Audits
 - i. Grantee understands and agrees that Grantee is subject to any and all applicable audit requirements found in state or federal law or regulation or added by this Grant Agreement
 - ii. HHS Single Audit Unit will notify Grantee to complete the Single Audit Determination Form. If Grantee fails to complete the form within thirty (30) calendar days after receipt of notice, Grantee maybe subject to sanctions and remedies for non-compliance.
 - iii. If Grantee, within Grantee's fiscal year, expends at least SEVEN HUNDRED FIFTY THOUSAND DOLLARS (\$750,000) in federal funds awarded, Grantee shall have a single audit or program-specific audit in accordance with 2 CFR 200. The federal threshold amount includes federal funds passed through by way of state agency awards.

- iv. If Grantee, within Grantee's fiscal year, expends at least SEVEN HUNDRED FIFTY THOUSAND DOLLARS (\$750,000) in state funds awarded, Grantee shall have a single audit or program-specific audit in accordance with TxGMS. The audit must be conducted by an independent certified public accountant and in accordance with 2 CFR 200, Government Auditing Standards, and TxGMS.
 - v. For-profit Grantees whose expenditures meet or exceed the federal or state expenditure thresholds stated above shall follow the guidelines in 2 CFR 200 or TxGMS, as applicable, for their program-specific audits.
 - vi. Each Grantee required to obtain a single audit must competitively re-procure single audit services once every six years. Grantee shall procure audit services in compliance with this section, state procurement procedures, as well as with applicable provisions of 2 CFR 200 and TxGMS.
- B. Financial Statements.
Each Grantee that does not meet the expenditure threshold for a single audit or program-specific audit, must provide financial statements for the audit period.

4.3 SUBMISSION OF AUDITS AND FINANCIAL STATEMENTS

- A. Audits.
Due the earlier of 30 days after receipt of the independent certified public accountant's report or nine months after the end of the fiscal year, Grantee shall submit one electronic copy of the single audit or program-specific audit to the System Agency via:
- i. HHS portal at <https://hhsportal.hhs.state.tx.us/heartwebextr/hhscSau> or,
 - ii. Email to: single_audit_report@hhsc.state.tx.us.
- B. Financial Statements.
Due no later than nine months after the Grantee's fiscal year-end, Grantees not required to submit an audit, shall submit one electronic copy of their financial statements via:
- i. HHS portal at <https://hhsportal.hhs.state.tx.us/heartwebextr/hhscSau>; or,
 - ii. Email to: single_audit_report@hhsc.state.tx.us.

ARTICLE V. WARRANTY, AFFIRMATIONS, ASSURANCES AND CERTIFICATIONS

5.1 WARRANTY

Grantee warrants that all work under this Grant Agreement shall be completed in a manner consistent with standards under the terms of this Grant Agreement, in the applicable trade, profession, or industry; shall conform to or exceed the specifications set forth in the Grant Agreement; and all deliverables shall be fit for ordinary use, of good quality, and with no material defects. If System Agency, in its sole discretion, determines Grantee has failed to complete work timely or to perform satisfactorily under conditions required by this Grant Agreement, the System Agency may require Grantee, at its sole expense, to:

- i. Repair or replace all defective or damaged work;
- ii. Refund any payment Grantee received from System Agency for all defective or damaged work and, in conjunction therewith, require Grantee to accept the return of such work; and,
- iii. Take necessary action to ensure that Grantee's future performance and work conform to the Grant Agreement requirements.

5.2 GENERAL AFFIRMATIONS

Grantee certifies that, to the extent affirmations are incorporated into the Grant Agreement, the Grantee has reviewed the affirmations and that Grantee is in compliance with all requirements.

5.3 FEDERAL ASSURANCES

Grantee further certifies that, to the extent federal assurances are incorporated into the Grant Agreement, the Grantee has reviewed the federal assurances and that Grantee is in compliance with all requirements.

5.4 FEDERAL CERTIFICATIONS

Grantee further certifies that, to the extent federal certifications are incorporated into the Grant Agreement, the Grantee has reviewed the federal certifications and that Grantee is in compliance with all requirements. In addition, Grantee certifies that it is in compliance with all applicable federal laws, rules, and regulations, as they may pertain to this Grant Agreement.

5.5 STATE ASSURANCES

Except to the extent of any conflict under applicable law or requirements or guidelines of any federal awarding agency from which funding for this Grant Agreement originated, the Grantee must comply with the applicable state assurances included within the TxGMS which are incorporated here by reference.

ARTICLE VI. INTELLECTUAL PROPERTY

6.1 OWNERSHIP OF WORK PRODUCT

- A. All right, title, and interest in the Work Product, including all Intellectual Property Rights therein, is exclusively owned by System Agency. Grantee and Grantee's employees will have no rights in or ownership of the Work Product or any other property of System Agency.
- B. Any and all Work Product that is copyrightable under United States copyright law is deemed to be "work made for hire" owned by System Agency, as provided by Title 17 of the United States Code. To the extent that Work Product does not qualify as a "work made for hire" under applicable federal law, Grantee hereby irrevocably assigns and transfers to System Agency, its successors and assigns, the entire right, title, and interest in and to the Work Product, including any and all Intellectual Property Rights embodied therein or associated therewith, and in and to all works based upon, derived from, or incorporating the Work Product, and in and to all income, royalties, damages, claims and payments now or hereafter due or payable with respect thereto, and in and to all causes of action, either in law or in equity for past, present or future infringement based on the copyrights, and in and to all rights corresponding to the foregoing.
- C. Grantee agrees to execute all papers and to perform such other acts as System Agency may deem necessary to secure for System Agency or its designee the rights herein assigned.
- D. In the event that Grantee has any rights in and to the Work Product that cannot be assigned to System Agency, Grantee hereby grants to System Agency an exclusive, worldwide, royalty-free, transferable, irrevocable, and perpetual license, with the right to

sublicense, to reproduce, distribute, modify, create derivative works of, publicly perform and publicly display, make, have made, use, sell and offer for sale the Work Product and any products developed by practicing such rights.

- E. The foregoing does not apply to Incorporated Pre-existing Works or Third Party IP that are incorporated in the Work Product by Grantee. Grantee shall provide System Agency access during normal business hours to all Grantee materials, premises, and computer files containing the Work Product.

6.2 GRANTEE'S PRE-EXISTING WORKS

- A. To the extent that Grantee incorporates into the Work Product any works of Grantee that were created by Grantee or that Grantee acquired rights in prior to the Effective Date of this Grant Agreement (“**Incorporated Pre-existing Works**”), Grantee retains ownership of such Incorporated Pre-existing Works.
- B. Grantee hereby grants to System Agency an irrevocable, perpetual, non-exclusive, royalty-free, transferable, worldwide right and license, with the right to sublicense, to use, reproduce, modify, copy, create derivative works of, publish, publicly perform and display, sell, offer to sell, make and have made, the Incorporated Pre-existing Works, in any medium, with or without the associated Work Product.
- C. Grantee represents, warrants, and covenants to System Agency that Grantee has all necessary right and authority to grant the foregoing license in the Incorporated Pre-existing Works to System Agency.

6.3 THIRD PARTY IP

- A. To the extent that any Third Party IP is included or incorporated in the Work Product by Grantee, Grantee hereby grants to System Agency, or shall obtain from the applicable third party for System Agency's benefit, the irrevocable, perpetual, non-exclusive, worldwide, royalty-free right and license, for System Agency's internal business or governmental purposes only, to use, reproduce, display, perform, distribute copies of, and prepare derivative works based upon such Third Party IP and any derivative works thereof embodied in or delivered to System Agency in conjunction with the Work Product, and to authorize others to do any or all of the foregoing.
- B. Grantee shall obtain System Agency's advance written approval prior to incorporating any Third Party IP into the Work Product, and Grantee shall notify System Agency on delivery of the Work Product if such materials include any Third Party IP.
- C. Grantee shall provide System Agency all supporting documentation demonstrating Grantee's compliance with this Section 6.3, including without limitation documentation indicating a third party's written approval for Grantee to use any Third Party IP that may be incorporated in the Work Product.

6.4 AGREEMENTS WITH EMPLOYEES AND SUBCONTRACTORS

Grantee shall have written, binding agreements with its employees and subcontractors that include provisions sufficient to give effect to and enable Grantee's compliance with Grantee's obligations under this Article VI, Intellectual Property.

6.5 DELIVERY UPON TERMINATION OR EXPIRATION

No later than the first calendar day after the termination or expiration of the Grant Agreement or upon System Agency's request, Grantee shall deliver to System Agency all completed, or

partially completed, Work Product, including any Incorporated Pre-existing Works, and any and all versions thereof. Grantee's failure to timely deliver such Work Product is a material breach of the Grant Agreement. Grantee will not retain any copies of the Work Product or any documentation or other products or results of Grantee's activities under the Grant Agreement without the prior written consent of System Agency.

6.6 SURVIVAL

The provisions and obligations of this Article survive any termination or expiration of the Grant Agreement.

6.7 SYSTEM AGENCY DATA

- A. As between the Parties, all data and information acquired, accessed, or made available to Grantee by, through, or on behalf of System Agency or System Agency contractors, including all electronic data generated, processed, transmitted, or stored by Grantee in the course of providing data processing services in connection with Grantee's performance hereunder (the "System Agency Data"), is owned solely by System Agency.
- B. Grantee has no right or license to use, analyze, aggregate, transmit, create derivatives of, copy, disclose, or process the System Agency Data except as required for Grantee to fulfill its obligations under the Grant Agreement or as authorized in advance in writing by System Agency.
- C. For the avoidance of doubt, Grantee is expressly prohibited from using, and from permitting any third party to use, System Agency Data for marketing, research, or other non-governmental or commercial purposes, without the prior written consent of System Agency.
- D. Grantee shall make System Agency Data available to System Agency, including to System Agency's designated vendors, as directed in writing by System Agency. The foregoing shall be at no cost to System Agency.
- E. Furthermore, the proprietary nature of Grantee's systems that process, store, collect, and/or transmit the System Agency Data shall not excuse Grantee's performance of its obligations hereunder.

ARTICLE VII. PROPERTY

7.1 USE OF STATE PROPERTY

- A. Grantee is prohibited from using State Property for any purpose other than performing Services authorized under the Grant Agreement.
- B. State Property includes, but is not limited to, System Agency's office space, identification badges, System Agency information technology equipment and networks (*e.g.*, laptops, portable printers, cell phones, iPads or tablets, external hard drives, data storage devices, any System Agency-issued software, and the System Agency Virtual Private Network (VPN client)), and any other resources of System Agency.
- C. Grantee shall not remove State Property from the continental United States. In addition, Grantee may not use any computing device to access System Agency's network or e-mail while outside of the continental United States.
- D. Grantee shall not perform any maintenance services on State Property unless the Grant Agreement expressly authorizes such Services.

- E. During the time that State Property is in the possession of Grantee, Grantee shall be responsible for:
 - i. all repair and replacement charges incurred by State Agency that are associated with loss of State Property or damage beyond normal wear and tear, and
 - ii. all charges attributable to Grantee's use of State Property that exceeds the Grant Agreement scope. Grantee shall fully reimburse such charges to System Agency within ten (10) calendar days of Grantee's receipt of System Agency's notice of amount due. Use of State Property for a purpose not authorized by the Grant Agreement shall constitute breach of contract and may result in termination of the Grant Agreement and the pursuit of other remedies available to System Agency under contract, at law, or in equity.

7.2 DAMAGE TO STATE PROPERTY

- A. In the event of loss, destruction, or damage to any System Agency or State of Texas owned, leased, or occupied property or equipment by Grantee or Grantee's employees, agents, Subcontractors, or suppliers, Grantee shall be liable to System Agency and the State of Texas for the full cost of repair, reconstruction, or replacement of the lost, destroyed, or damaged property.
- B. Grantee shall notify System Agency of the loss, destruction, or damage of equipment or property within one (1) business day. Grantee shall reimburse System Agency and the State of Texas for such property damage within ten (10) calendar days after Grantee's receipt of System Agency's notice of amount due.

7.3 PROPERTY RIGHTS UPON TERMINATION OR EXPIRATION OF CONTRACT

In the event the Grant Agreement is terminated for any reason or expires, State Property remains the property of the System Agency and must be returned to the System Agency by the earlier of the end date of the Grant Agreement or upon System Agency's request.

7.4 EQUIPMENT AND PROPERTY

- A. The Grantee must ensure equipment with a per-unit cost of \$5,000 or greater purchased with grant funds under this award is used solely for the purpose of this Grant or is properly pro-rated for use under this Grant. Grantee must have control systems to prevent loss, damage, or theft of property funded under this Grant. Grantee shall maintain equipment management and inventory procedures for equipment, whether acquired in part or whole with grant funds, until disposition occurs.
- B. When equipment acquired by Grantee under this Grant Agreement is no longer needed for the original project or for other activities currently supported by System Agency, the Grantee must properly dispose of the equipment pursuant to 2 CFR and/or TxGMS, as applicable. Upon termination of this Grant Agreement, use and disposal of equipment by the Grantee shall conform with TxGMS requirements.
- C. Grantee shall initiate the purchase of all equipment approved in writing by the System Agency in accordance with the schedule approved by System Agency, as applicable. Failure to timely initiate the purchase of equipment may result in the loss of availability of funds for the purchase of equipment. Requests to purchase previously approved equipment after the first quarter in the Grant Agreement must be submitted to the assigned System Agency contract manager.
- D. Controlled Assets include firearms, regardless of the acquisition cost, and the following

assets with an acquisition cost of \$500 or more, but less than \$5,000: desktop and laptop computers (including notebooks, tablets and similar devices), non-portable printers and copiers, emergency management equipment, communication devices and systems, medical and laboratory equipment, and media equipment. Controlled Assets are considered supplies.

- E. System Agency funds must not be used to purchase buildings or real property without prior written approval from System Agency. Any costs related to the initial acquisition of the buildings or real property are not allowable without written pre-approval.

ARTICLE VIII. RECORD RETENTION, AUDIT, AND CONFIDENTIALITY

8.1 RECORD MAINTENANCE AND RETENTION

- A. Grantee shall keep and maintain under GAAP or GASB, as applicable, full, true, and complete records necessary to fully disclose to the System Agency, the Texas State Auditor's Office, the United States Government, and their authorized representatives sufficient information to determine compliance with the terms and conditions of this Grant Agreement and all state and federal rules, regulations, and statutes.
- B. Grantee shall maintain and retain legible copies of this Grant Agreement and all records relating to the performance of the Grant Agreement, including supporting fiscal documents adequate to ensure that claims for grant funds are in accordance with applicable State of Texas requirements. These records shall be maintained and retained by the Grantee for a minimum of seven (7) years after the Grant Agreement expiration date or seven (7) years after all audits, claims, litigation or disputes involving the Grant Agreement are resolved, whichever is later.

8.2 AGENCY'S RIGHT TO AUDIT

- A. Grantee shall make available at reasonable times and upon reasonable notice, and for reasonable periods, work papers, reports, books, records, supporting documents kept current by Grantee pertaining to the Grant Agreement for purposes of inspecting, monitoring, auditing, or evaluating by System Agency and the State of Texas.
- B. In addition to any right of access arising by operation of law, Grantee and any of Grantee's affiliate or subsidiary organizations, or Subcontractors shall permit the System Agency or any of its duly authorized representatives, as well as duly authorized federal, state or local authorities, unrestricted access to and the right to examine any site where business is conducted or services are performed, and all records, which includes but is not limited to financial, client and patient records, books, papers or documents related to this Grant Agreement. If the Grant Agreement includes federal funds, federal agencies that shall have a right of access to records as described in this section include: the federal agency providing the funds, the Comptroller General of the United States, the General Accounting Office, the Office of the Inspector General, and any of their authorized representatives. In addition, agencies of the State of Texas that shall have a right of access to records as described in this section include: the System Agency, HHS's contracted examiners, the State Auditor's Office, the Office of the Texas Attorney General, and any successor agencies. Each of these entities may be a duly authorized authority.

- C. If deemed necessary by the System Agency or any duly authorized authority, for the purpose of investigation or hearing, Grantee shall produce original documents related to this Grant Agreement.
- D. The System Agency and any duly authorized authority shall have the right to audit billings both before and after payment, and all documentation that substantiates the billings.
- E. Grantee shall include this provision concerning the right of access to, and examination of, sites and information related to this Grant Agreement in any Subcontract it awards.

8.3 RESPONSE/COMPLIANCE WITH AUDIT OR INSPECTION FINDINGS

- A. Grantee must act to ensure its and its Subcontractors' compliance with all corrections necessary to address any finding of noncompliance with any law, regulation, audit requirement, or generally accepted accounting principle, or any other deficiency identified in any audit, review, or inspection of the Grant Agreement and the services and Deliverables provided. Any such correction will be at Grantee's or its Subcontractor's sole expense. Whether Grantee's action corrects the noncompliance shall be solely the decision of the System Agency.
- B. As part of the services, Grantee must provide to HHS upon request a copy of those portions of Grantee's and its Subcontractors' internal audit reports relating to the services and Deliverables provided to the State under the Grant Agreement.

8.4 STATE AUDITOR'S RIGHT TO AUDIT

The state auditor may conduct an audit or investigation of any entity receiving funds from the state directly under the Grant Agreement or indirectly through a subcontract under the Grant Agreement. The acceptance of funds directly under the Grant Agreement or indirectly through a subcontract under the Grant Agreement acts as acceptance of the authority of the state auditor, under the direction of the legislative audit committee, to conduct an audit or investigation in connection with those funds. Under the direction of the legislative audit committee, an entity that is the subject of an audit or investigation by the state auditor must provide the state auditor with access to any information the state auditor considers relevant to the investigation or audit.

8.5 CONFIDENTIALITY

Grantee shall maintain as confidential and shall not disclose to third parties without System Agency's prior written consent, any System Agency information including but not limited to System Agency's business activities, practices, systems, conditions and services. This section will survive termination or expiration of this Grant Agreement. This requirement must be included in all subcontracts awarded by Grantee.

ARTICLE IX. GRANT REMEDIES, TERMINATION AND PROHIBITED ACTIVITIES

9.1 REMEDIES

- A. To ensure Grantee's full performance of the Grant Agreement and compliance with applicable law, System Agency reserves the right to hold Grantee accountable for breach of contract or substandard performance and may take remedial or corrective actions,

including, but not limited to the following:

- i. temporarily withholding cash disbursements or reimbursements pending correction of the deficiency;
 - ii. disallowing or denying use of funds for the activity or action deemed not to be in compliance;
 - iii. disallowing claims for reimbursement that may require a partial or whole return of previous payments or reimbursements;
 - iv. suspending all or part of the Grant Agreement;
 - v. requiring the Grantee to take specific actions in order to remain in compliance with the Grant Agreement;
 - vi. recouping payments made by the System Agency to the Grantee found to be in error;
 - vii. suspending, limiting, or placing conditions on the Grantee's continued performance of the Project;
 - viii. prohibiting the Grantee from receiving additional funds for other grant programs administered by the System Agency until satisfactory compliance resolution is obtained;
 - ix. withholding release of new grant agreements; and
 - x. imposing any other remedies, sanctions or penalties authorized under this Grant Agreement or permitted by federal or state statute, law, regulation or rule.
- B. Unless expressly authorized by System Agency, Grantee may not be entitled to reimbursement for expenses incurred while the Grant Agreement is suspended.
- C. No action taken by System Agency in exercising remedies or imposing sanctions will constitute or operate as a waiver of any other rights or remedies available to System Agency under the Grant Agreement or pursuant to law. Additionally, no action taken by System Agency in exercising remedies or imposing sanctions will constitute or operate as an acceptance, waiver, or cure of Grantee's breach. Unless expressly authorized by System Agency, Grantee may not be entitled to reimbursement for expenses incurred while the Grant Agreement is suspended or after termination.

9.2 TERMINATION FOR CONVENIENCE

The System Agency may terminate the Grant Agreement, in whole or in part, at any time when, in its sole discretion, the System Agency determines that termination is in the best interests of the State of Texas. The termination will be effective on the date specified in the System Agency's notice of termination.

9.3 TERMINATION FOR CAUSE

- A. Except as otherwise provided by the U.S. Bankruptcy Code, or any successor law, the System Agency may terminate the Grant Agreement, in whole or in part, upon either of the following conditions:

i. Material Breach

The System Agency may terminate the Grant Agreement, in whole or in part, if the System Agency determines, in its sole discretion, that Grantee has materially breached the Grant Agreement or has failed to adhere to any laws, ordinances, rules, regulations or orders of any public authority having jurisdiction, whether or not such violation prevents or substantially impairs performance of Grantee's duties under the Grant Agreement. Grantee's misrepresentation in any aspect including, but not limited to, of Grantee's Solicitation Application, if any, or Grantee's

addition to the SAM exclusion list (identification in SAM as an excluded entity) may also constitute a material breach of the Grant Agreement.

ii. Failure to Maintain Financial Viability

The System Agency may terminate the Grant Agreement if the System Agency, in its sole discretion, determines that Grantee no longer maintains the financial viability required to complete the services and deliverables, or otherwise fully perform its responsibilities under the Grant Agreement.

- B. System Agency will specify the effective date of such termination in the notice to Grantee. If no effective date is specified, the Grant Agreement will terminate on the date of the notification.

9.4 GRANTEE RESPONSIBILITY FOR SYSTEM AGENCY'S TERMINATION COSTS

If the System Agency terminates the Grant Agreement for cause, the Grantee shall be responsible to the System Agency for all costs incurred by the System Agency and the State of Texas to replace the Grantee. These costs include, but are not limited to, the costs of procuring a substitute grantee and the cost of any claim or litigation attributable to Grantee's failure to perform any work in accordance with the terms of the Grant Agreement.

9.5 INHERENTLY RELIGIOUS ACTIVITIES

Grantee may not use grant funding to engage in inherently religious activities, such as proselytizing, scripture study, or worship. Grantees may engage in inherently religious activities; however, these activities must be separate in time or location from the grant-funded program. Moreover, grantees must not compel program beneficiaries to participate in inherently religious activities. These requirements apply to all grantees, not just faith-based organizations.

9.6 POLITICAL ACTIVITIES

Grant funds cannot be used for the following activities:

- A. Grantees and their relevant sub-grantees or subcontractors are prohibited from using grant funds directly or indirectly for political purposes, including lobbying, advocating for legislation, campaigning for, endorsing, contributing to, or otherwise supporting political candidates or parties, and voter registration campaigns. Grantees may use private, or non-System Agency money or contributions for political purposes but may not charge to, or be reimbursed from, System Agency contracts or grants for the costs of such activities.
- B. Grant-funded employees may not use official authority or influence to achieve any political purpose and grant funds cannot be used for the salary, benefits, or any other compensation of an elected official.
- C. Grant funds may not be used to employ, in any capacity, a person who is required by Chapter 305 of the Texas Government Code to register as a lobbyist. Additionally, grant funds cannot be used to pay membership dues to an organization that partially or wholly pays the salary of a person who is required by Chapter 305 of the Texas Government Code to register as a lobbyist.
- D. As applicable, Grantee will comply with 31 USC § 1352, relating to the limitation on use of appropriated funds to influence certain Federal contracting and financial transactions.

ARTICLE X. INDEMNITY

10.1 GENERAL INDEMNITY

- A. GRANTEE SHALL DEFEND, INDEMNIFY AND HOLD HARMLESS THE STATE OF TEXAS AND SYSTEM AGENCY, AND/OR THEIR OFFICERS, AGENTS, EMPLOYEES, REPRESENTATIVES, CONTRACTORS, ASSIGNEES, AND/OR DESIGNEES FROM ANY AND ALL LIABILITY, ACTIONS, CLAIMS, DEMANDS, OR SUITS, AND ALL RELATED COSTS, ATTORNEYS' FEES, AND EXPENSES ARISING OUT OF OR RESULTING FROM ANY ACTS OR OMISSIONS OF GRANTEE OR ITS AGENTS, EMPLOYEES, SUBCONTRACTORS, ORDER FULFILLERS, OR SUPPLIERS OF SUBCONTRACTORS IN THE EXECUTION OR PERFORMANCE OF THE GRANT AGREEMENT AND ANY PURCHASE ORDERS ISSUED UNDER THE GRANT AGREEMENT.
- B. THIS PARAGRAPH IS NOT INTENDED TO AND WILL NOT BE CONSTRUED TO REQUIRE GRANTEE TO INDEMNIFY OR HOLD HARMLESS THE STATE OR THE SYSTEM AGENCY FOR ANY CLAIMS OR LIABILITIES RESULTING FROM THE NEGLIGENT ACTS OF OMISSIONS OF THE SYSTEM AGENCY OR ITS EMPLOYEES.
- C. For the avoidance of doubt, System Agency shall not indemnify Grantee or any other entity under the Grant Agreement.

10.2 INTELLECTUAL PROPERTY

GRANTEE SHALL DEFEND, INDEMNIFY, AND HOLD HARMLESS THE SYSTEM AGENCY AND THE STATE OF TEXAS FROM AND AGAINST ANY AND ALL CLAIMS, VIOLATIONS, MISAPPROPRIATIONS, OR INFRINGEMENT OF ANY PATENT, TRADEMARK, COPYRIGHT, TRADE SECRET, OR OTHER INTELLECTUAL PROPERTY RIGHTS AND/OR OTHER INTANGIBLE PROPERTY, PUBLICITY OR PRIVACY RIGHTS, AND/OR IN CONNECTION WITH OR ARISING FROM:

- i. THE PERFORMANCE OR ACTIONS OF GRANTEE PURSUANT TO THIS GRANT AGREEMENT;
- ii. ANY DELIVERABLE, WORK PRODUCT, CONFIGURED SERVICE OR OTHER SERVICE PROVIDED HEREUNDER; AND/OR
- iii. SYSTEM AGENCY'S AND/OR GRANTEE'S USE OF OR ACQUISITION OF ANY REQUESTED SERVICES OR OTHER ITEMS PROVIDED TO SYSTEM AGENCY BY GRANTEE OR OTHERWISE TO WHICH SYSTEM AGENCY HAS ACCESS AS A RESULT OF GRANTEE'S PERFORMANCE UNDER THE GRANT AGREEMENT.

10.3 ADDITIONAL INDEMNITY PROVISIONS

- A. GRANTEE AND SYSTEM AGENCY AGREE TO FURNISH TIMELY WRITTEN NOTICE TO EACH OTHER OF ANY INDEMNITY CLAIM. GRANTEE SHALL BE LIABLE TO PAY ALL COSTS OF DEFENSE, INCLUDING ATTORNEYS' FEES.
- B. THE DEFENSE SHALL BE COORDINATED BY THE GRANTEE WITH THE

OFFICE OF THE TEXAS ATTORNEY GENERAL WHEN TEXAS STATE AGENCIES ARE NAMED DEFENDANTS IN ANY LAWSUIT AND GRANTEE MAY NOT AGREE TO ANY SETTLEMENT WITHOUT FIRST OBTAINING THE CONCURRENCE FROM THE OFFICE OF THE TEXAS ATTORNEY GENERAL.

- C. GRANTEE SHALL REIMBURSE SYSTEM AGENCY AND THE STATE OF TEXAS FOR ANY CLAIMS, DAMAGES, COSTS, EXPENSES OR OTHER AMOUNTS, INCLUDING, BUT NOT LIMITED TO, ATTORNEYS' FEES AND COURT COSTS, ARISING FROM ANY SUCH CLAIM. IF THE SYSTEM AGENCY DETERMINES THAT A CONFLICT EXISTS BETWEEN ITS INTERESTS AND THOSE OF GRANTEE OR IF SYSTEM AGENCY IS REQUIRED BY APPLICABLE LAW TO SELECT SEPARATE COUNSEL, SYSTEM AGENCY WILL BE PERMITTED TO SELECT SEPARATE COUNSEL AND GRANTEE SHALL PAY ALL REASONABLE COSTS OF SYSTEM AGENCY'S COUNSEL.**

ARTICLE XI. GENERAL PROVISIONS

11.1 AMENDMENTS

Except as otherwise expressly provided, the Grant Agreement may only be amended by a written Amendment executed by both Parties.

11.2 NO QUANTITY GUARANTEES

The System Agency makes no guarantee of volume or usage of work under this Grant Agreement. All work requested may be on an irregular and as needed basis throughout the Grant Agreement term.

11.3 CHILD ABUSE REPORTING REQUIREMENTS

- A. Grantees shall comply with child abuse and neglect reporting requirements in Texas Family Code Chapter 261. This section is in addition to and does not supersede any other legal obligation of the Grantee to report child abuse.
- B. Grantee shall develop, implement and enforce a written policy that includes at a minimum the System Agency's Child Abuse Screening, Documenting, and Reporting Policy for Grantees/Providers and train all staff on reporting requirements.
- C. Grantee shall use the Texas Abuse Hotline Website located at <https://www.txabusehotline.org/Login/Default.aspx> as required by the System Agency. Grantee shall retain reporting documentation on site and make it available for inspection by the System Agency.

11.4 CERTIFICATION OF MEETING OR EXCEEDING TOBACCO-FREE WORKPLACE POLICY MINIMUM STANDARDS

- A. Grantee certifies that it has adopted and enforces a Tobacco-Free Workplace Policy that meets or exceeds all of the following minimum standards of:
 - i. Prohibiting the use of all forms of tobacco products, including but not limited to cigarettes, cigars, pipes, water pipes (hookah), bidis, kreteks, electronic cigarettes, smokeless tobacco, snuff and chewing tobacco;

- ii. Designating the property to which this Policy applies as a "designated area," which must at least comprise all buildings and structures where activities funded under this Grant Agreement are taking place, as well as Grantee owned, leased, or controlled sidewalks, parking lots, walkways, and attached parking structures immediately adjacent to this designated area;
 - iii. Applying to all employees and visitors in this designated area; and
 - iv. Providing for or referring its employees to tobacco use cessation services.
- B. If Grantee cannot meet these minimum standards, it must obtain a waiver from the System Agency.

11.5 INSURANCE AND BONDS

Unless otherwise specified in this Contract, Grantee shall acquire and maintain, for the duration of this Contract, insurance coverage necessary to ensure proper fulfillment of this Contract and potential liabilities thereunder with financially sound and reputable insurers licensed by the Texas Department of Insurance, in the type and amount customarily carried within the industry as determined by the System Agency. Grantee shall provide evidence of insurance as required under this Contract, including a schedule of coverage or underwriter's schedules establishing to the satisfaction of the System Agency the nature and extent of coverage granted by each such policy, upon request by the System Agency. In the event that any policy is determined by the System Agency to be deficient to comply with the terms of this Contract, Grantee shall secure such additional policies or coverage as the System Agency may reasonably request or that are required by law or regulation. If coverage expires during the term of this Contract, Grantee must produce renewal certificates for each type of coverage. In addition, if required by System Agency, Grantee must obtain and have on file a blanket fidelity bond that indemnifies System Agency against the loss or theft of any grant funds, including applicable matching funds. The fidelity bond must cover the entirety of the grant term and any subsequent renewals. The failure of Grantee to comply with these requirements may subject Grantee to remedial or corrective actions detailed in section 10.1, General Indemnity, above.

These and all other insurance requirements under the Grant apply to both Grantee and its Subcontractors, if any. Grantee is responsible for ensuring its Subcontractors' compliance with all requirements.

11.6 LIMITATION ON AUTHORITY

- A. Grantee shall not have any authority to act for or on behalf of the System Agency or the State of Texas except as expressly provided for in the Grant Agreement; no other authority, power, or use is granted or implied. Grantee may not incur any debt, obligation, expense, or liability of any kind on behalf of System Agency or the State of Texas.
- B. Grantee may not rely upon implied authority and is not granted authority under the Grant Agreement to:
- i. Make public policy on behalf of the System Agency;
 - ii. Promulgate, amend, or disregard administrative regulations or program policy decisions made by State and federal agencies responsible for administration of a System Agency program; or
 - iii. Unilaterally communicate or negotiate with any federal or state agency or the Texas

Legislature on behalf of the System Agency regarding System Agency programs or the Grant Agreement. However, upon System Agency request and with reasonable notice from System Agency to the Grantee, the Grantee shall assist the System Agency in communications and negotiations regarding the Work under the Grant Agreement with state and federal governments.

11.7 CHANGE IN LAWS AND COMPLIANCE WITH LAWS

Grantee shall comply with all laws, regulations, requirements and guidelines applicable to a Grantee providing services and products required by the Grant Agreement to the State of Texas, as these laws, regulations, requirements and guidelines currently exist and as amended throughout the term of the Grant Agreement. Notwithstanding Section 11.1, Amendments, above, System Agency reserves the right, in its sole discretion, to unilaterally amend the Grant Agreement to incorporate any modifications necessary for System Agency's compliance, as an agency of the State of Texas, with all applicable state and federal laws, regulations, requirements and guidelines.

11.8 SUBCONTRACTORS

Grantee may not subcontract any or all of the Work and/or obligations under the Grant Agreement without prior written approval of the System Agency. Subcontracts, if any, entered into by the Grantee shall be in writing and be subject to the requirements of the Grant Agreement. Should Grantee subcontract any of the services required in the Grant Agreement, Grantee expressly understands and acknowledges System Agency is in no manner liable to any subcontractor(s) of Grantee. In no event shall this provision relieve Grantee of the responsibility for ensuring that the services performed under all subcontracts are rendered in compliance with the Grant Agreement.

11.9 PERMITTING AND LICENSURE

At Grantee's sole expense, Grantee shall procure and maintain for the duration of this Grant Agreement any state, county, city, or federal license, authorization, insurance, waiver, permit, qualification or certification required by statute, ordinance, law, or regulation to be held by Grantee to provide the goods or services required by this Grant Agreement. Grantee shall be responsible for payment of all taxes, assessments, fees, premiums, permits, and licenses required by law. Grantee shall be responsible for payment of any such government obligations not paid by its Subcontractors during performance of this Grant Agreement.

11.10 INDEPENDENT CONTRACTOR

Grantee and Grantee's employees, representatives, agents, Subcontractors, suppliers, and third-party service providers shall serve as independent contractors in providing the services under the Grant Agreement. Neither Grantee nor System Agency is an agent of the other and neither may make any commitments on the other party's behalf. The Grantee is not a "governmental body" solely by virtue of this Grant Agreement or receipt of grant funds under this Grant Agreement. Grantee shall have no claim against System Agency for vacation pay, sick leave, retirement benefits, social security, worker's compensation, health or disability benefits, unemployment insurance benefits, or employee benefits of any kind. The Grant Agreement shall not create any joint venture, partnership, agency, or employment relationship between Grantee and System Agency.

11.11 GOVERNING LAW AND VENUE

The Grant Agreement shall be governed by and construed in accordance with the laws of the State of Texas, without regard to the conflicts of law provisions. The venue of any suit arising under the Grant Agreement is fixed in any court of competent jurisdiction of Travis County, Texas, unless the specific venue is otherwise identified in a statute which directly names or otherwise identifies its applicability to the System Agency.

11.12 SEVERABILITY

If any provision contained in this Grant Agreement is held to be unenforceable by a court of law or equity, such construction will not affect the legality, validity, or enforceability of any other provision or provisions of this Grant Agreement. It is the intent and agreement of the Parties this Grant Agreement shall be deemed amended by modifying such provision to the extent necessary to render it valid, legal and enforceable while preserving its intent or, if such modification is not possible, by substituting another provision that is valid, legal and enforceable and that achieves the same objective. All other provisions of this Grant Agreement will continue in full force and effect.

11.13 SURVIVABILITY

Expiration or termination of the Grant Agreement for any reason does not release Grantee from any liability or obligation set forth in the Grant Agreement that is expressly stated to survive any such expiration or termination, that by its nature would be intended to be applicable following any such expiration or termination, or that is necessary to fulfill the essential purpose of the Grant Agreement, including without limitation the provisions regarding return of grant funds, audit requirements, records retention, public information, warranty, indemnification, confidentiality, and rights and remedies upon termination.

11.14 FORCE MAJEURE

Neither Grantee nor System Agency shall be liable to the other for any delay in, or failure of performance, of any requirement included in the Grant Agreement caused by force majeure. The existence of such causes of delay or failure shall extend the period of performance until after the causes of delay or failure have been removed provided the non-performing party exercises all reasonable due diligence to perform. Force majeure is defined as acts of God, war, fires, explosions, hurricanes, floods, failure of transportation, or other causes that are beyond the reasonable control of either party and that by exercise of due foresight such party could not reasonably have been expected to avoid, and which, by the exercise of all reasonable due diligence, such party is unable to overcome.

11.15 NO IMPLIED WAIVER OF PROVISIONS

The failure of the System Agency to object to or to take affirmative action with respect to any conduct of the Grantee which is in violation or breach of the terms of the Grant Agreement shall not be construed as a waiver of the violation or breach, or of any future violation or breach.

11.16 FUNDING DISCLAIMERS AND LABELING

A. Grantee shall not use System Agency's name or refer to System Agency directly or indirectly in any media appearance, public service announcement, or disclosure relating to this Grant Agreement including any promotional material without first obtaining

written consent from System Agency. The foregoing prohibition includes, without limitation, the placement of banners, pop-up ads, or other advertisements promoting Grantee's or a third party's products, services, workshops, trainings, or other commercial offerings on any website portal or internet-based service or software application hosted or managed by Grantee. This does not limit the Grantee's responsibility to comply with obligations related to the Texas Public Information Act or Texas Open Meetings Act.

- B. In general, no publication (including websites, reports, projects, etc.) may convey System Agency's recognition or endorsement of the Grantee's project without prior written approval from System Agency. Publications funded in part or wholly by HHS grant funding must include a statement that "HHS and neither any of its components operate, control, are responsible for, or necessarily endorse, this publication (including, without limitation, its content, technical infrastructure, and policies, and any services or tools provided)" at HHS's request.

11.17 MEDIA RELEASES

- A. Grantee shall not use System Agency's name, logo, or other likeness in any press release, marketing material or other announcement without System Agency's prior written approval. System Agency does not endorse any vendor, commodity, or service. Grantee is not authorized to make or participate in any media releases or public announcements pertaining to this Grant Agreement or the Services to which they relate without System Agency's prior written consent, and then only in accordance with explicit written instruction from System Agency.
- B. Grantee may publish, at its sole expense, results of Grantee performance under the Grant Agreement with the System Agency's prior review and approval, which the System Agency may exercise at its sole discretion. Any publication (written, visual, or sound) will acknowledge the support received from the System Agency and any Federal agency, as appropriate.

11.18 PROHIBITION ON NON-COMPETE RESTRICTIONS

Grantee shall not require any employees or Subcontractors to agree to any conditions, such as non-compete clauses or other contractual arrangements, that would limit or restrict such persons or entities from employment or contracting with the State of Texas.

11.19 SOVEREIGN IMMUNITY

Nothing in the Grant Agreement will be construed as a waiver of the System Agency's or the State's sovereign immunity. This Grant Agreement shall not constitute or be construed as a waiver of any of the privileges, rights, defenses, remedies, or immunities available to the System Agency or the State of Texas. The failure to enforce, or any delay in the enforcement, of any privileges, rights, defenses, remedies, or immunities available to the System Agency or the State of Texas under the Grant Agreement or under applicable law shall not constitute a waiver of such privileges, rights, defenses, remedies, or immunities or be considered as a basis for estoppel. System Agency does not waive any privileges, rights, defenses, or immunities available to System Agency by entering into the Grant Agreement or by its conduct prior to or subsequent to entering into the Grant Agreement.

11.20 ENTIRE CONTRACT AND MODIFICATION

The Grant Agreement constitutes the entire agreement of the Parties and is intended as a complete and exclusive statement of the promises, representations, negotiations, discussions, and other agreements that may have been made in connection with the subject matter hereof. Any additional or conflicting terms in any future document incorporated into the Grant Agreement will be harmonized with this Grant Agreement to the extent possible.

11.21 COUNTERPARTS

This Grant Agreement may be executed in any number of counterparts, each of which will be an original, and all such counterparts will together constitute but one and the same Grant Agreement.

11.22 PROPER AUTHORITY

Each Party represents and warrants that the person executing this Grant Agreement on its behalf has full power and authority to enter into this Grant Agreement.

11.23 E-VERIFY PROGRAM

Grantee certifies that it utilizes and will continue to utilize the U.S. Department of Homeland Security's E-Verify system to determine the eligibility of:

- A. all persons employed to perform duties within Texas during the term of the Grant Agreement; and
- B. all persons, (including subcontractors) assigned by the Grantee to perform work pursuant to the Grant Agreement within the United States of America.

11.24 CIVIL RIGHTS

- A. Grantee agrees to comply with state and federal anti-discrimination laws, including:
 - i. Title VI of the Civil Rights Act of 1964 (42 U.S.C. §2000d et seq.);
 - ii. Section 504 of the Rehabilitation Act of 1973 (29 U.S.C. §794);
 - iii. Americans with Disabilities Act of 1990 (42 U.S.C. §12101 et seq.);
 - iv. Age Discrimination Act of 1975 (42 U.S.C. §§6101-6107);
 - v. Title IX of the Education Amendments of 1972 (20 U.S.C. §§1681-1688);
 - vi. Food and Nutrition Act of 2008 (7 U.S.C. §2011 et seq.); and
 - vii. The System Agency's administrative rules, as set forth in the Texas Administrative Code, to the extent applicable to this Grant Agreement.
- B. Grantee agrees to comply with all amendments to the above-referenced laws, and all requirements imposed by the regulations issued pursuant to these laws. These laws provide in part that no persons in the United States may, on the grounds of race, color, national origin, sex, age, disability, political beliefs, or religion, be excluded from participation in or denied any aid, care, service or other benefits provided by Federal or State funding, or otherwise be subjected to discrimination.
- C. Grantee agrees to comply with Title VI of the Civil Rights Act of 1964, and its implementing regulations at 45 C.F.R. Part 80 or 7 C.F.R. Part 15, prohibiting a contractor from adopting and implementing policies and procedures that exclude or have the effect of excluding or limiting the participation of clients in its programs, benefits, or activities on the basis of national origin. State and federal civil rights laws require contractors to provide alternative methods for ensuring access to services for applicants and recipients who cannot express themselves fluently in English. Grantee agrees to take

reasonable steps to provide services and information, both orally and in writing, in appropriate languages other than English, in order to ensure that persons with limited English proficiency are effectively informed and can have meaningful access to programs, benefits, and activities.

- D. Grantee agrees to post applicable civil rights posters in areas open to the public informing clients of their civil rights and including contact information for the HHS Civil Rights Office. The posters are available on the HHS website at: <https://hhs.texas.gov/about-hhs/your-rights/civil-rights-office/civil-rights-posters>.
- E. Grantee agrees to comply with Executive Order 13279, and its implementing regulations at 45 C.F.R. Part 87 or 7 C.F.R. Part 16. These provide in part that any organization that participates in programs funded by direct financial assistance from the United States Department of Agriculture or the United States Department of Health and Human Services shall not discriminate against a program beneficiary or prospective program beneficiary on the basis of religion or religious belief.
- F. Upon request, Grantee shall provide HHSC's Civil Rights Office with copies of the Grantee's civil rights policies and procedures.
- G. Grantee must notify HHSC's Civil Rights Office of any complaints of discrimination received relating to its performance under this Grant Agreement. This notice must be delivered no more than ten (10) calendar days after receipt of a complaint. Notice provided pursuant to this section must be directed to:

HHSC Civil Rights Office
701 W. 51st Street, Mail Code W206
Austin, Texas 78751
Phone Toll Free: (888) 388-6332
Phone: (512) 438-4313
Fax: (512) 438-5885
Email: HHSCivilRightsOffice@hhsc.state.tx.us.

11.25 ENTERPRISE INFORMATION MANAGEMENT STANDARDS

Grantee shall conform to HHS standards for data management as described by the policies of the HHS Chief Data and Analytics Officer. These include, but are not limited to, standards for documentation and communication of data models, metadata, and other data definition methods that are required by HHS for ongoing data governance, strategic portfolio analysis, interoperability planning, and valuation of HHS System data assets.

11.26 DISCLOSURE OF LITIGATION

- A. The Grantee must disclose in writing to the contract manager assigned to this Grant Agreement any material civil or criminal litigation or indictment either threatened or pending involving the Grantee. "Threatened litigation" as used herein shall include governmental investigations and civil investigative demands. "Litigation" as used herein shall include administrative enforcement actions brought by governmental agencies. The Grantee must also disclose any material litigation threatened or pending involving Subcontractors, consultants, and/or lobbyists. For purposes of this section, "material" refers, but is not limited, to any action or pending action that a reasonable person knowledgeable in the applicable industry would consider relevant to the Work under the Grant Agreement or any development such a person would want to be aware of in order to stay fully apprised of the total mix of information relevant to the Work, together with

any litigation threatened or pending that may result in a substantial change in the Grantee's financial condition.

- B. This is a continuing disclosure requirement; any litigation commencing after Grant Agreement Award must be disclosed in a written statement to the assigned contract manager within seven calendar days of its occurrence.

11.27 NO THIRD PARTY BENEFICIARIES

The Grant Agreement is made solely and specifically among and for the benefit of the Parties named herein and their respective successors and assigns, and no other person shall have any right, interest, or claims hereunder or be entitled to any benefits pursuant to or on account of the Grant Agreement as a third-party beneficiary or otherwise.

11.28 BINDING EFFECT

The Grant Agreement shall inure to the benefit of, be binding upon, and be enforceable against each Party and their respective permitted successors, assigns, transferees, and delegates.



TEXAS

Health and Human Services

**Health and Human Services (HHS)
Additional Provisions
Version 1.0
Effective: November 7, 2019**

Table of Contents

1.^{na} NOTICE OF CRIMINAL ACTIVITY AND DISCIPLINARY ACTIONS..... 1

2. DISASTER SERVICES 1

3.^{na} NOTICE OF CONTRACT ACTION 1

4. NOTICE OF BANKRUPTCY..... 2

5.^{na} CONTRACTOR NOTIFICATION OF CHANGE OF CONTACT PERSON OR KEY PERSONNEL 2

7. THIRD PARTY PAYORS 2

8. HIV/AIDS MODEL WORKPLACE GUIDELINES 3

9. MEDICAL RECORDS RETENTION..... 3

10. ^{DocuSigned by:} NOTICE OF A LICENSE ACTION..... May 16, 2022 3
Steven Viera

11. ~~INTERIM~~ EXTENSION AMENDMENT 3

12.^{na} CONTRACTOR'S CERTIFICATION OF MEETING OR EXCEEDING TABACCO-FREE WORKPLACE POLICY MINIMUM STANDARDS 4

na

na

na

na

na

na

na

na

na

na

na

na

ADDITIONAL PROVISIONS

The terms and conditions of these Additional Provisions are incorporated into and made a part of the Contract. Capitalized items used in these Additional Provisions and not otherwise defined have the meanings assigned to them in HHSC Uniform Terms and Conditions.

1. NOTICE OF CRIMINAL ACTIVITY AND DISCIPLINARY ACTIONS

- A. Grantee shall immediately report in writing to its assigned HHSC contract manager when Grantee learns of or has any reason to believe it or any person with ownership or controlling interest in Grantee, or their agent, employee, subcontractor or volunteer who is providing services under this Contract has:
 - i. Engaged in any activity that could constitute a criminal offense equal to or greater than a Class A misdemeanor or grounds for disciplinary action by a state or federal regulatory authority; or
 - ii. Been placed on community supervision, received deferred adjudication, or been indicted for or convicted of a criminal offense relating to involvement in any financial matter, federal or state program or felony sex crime.
- B. Grantee shall not permit any person who engaged, or was alleged to have engaged, in any activity subject to reporting under this section to perform direct client services or have direct contact with clients, unless otherwise directed in writing by the System Agency.

2. DISASTER SERVICES

In the event of a local, state, or federal emergency, including natural, man-made, criminal, terrorist, and/or bioterrorism events, declared as a state disaster by the Governor, or a federal disaster declared by the appropriate federal official, Grantee may be called upon to assist the System Agency in providing the following services:

- i. Community evacuation;
- ii. Health and medical assistance;
- iii. Assessment of health and medical needs;
- iv. Health surveillance;
- v. Medical care personnel;
- vi. Health and medical equipment and supplies;
- vii. Patient evacuation;
- viii. In-hospital care and hospital facility status;
- ix. Food, drug and medical device safety;
- x. Worker health and safety;
- xi. Mental health and substance abuse;
- xii. Public health information;
- xiii. Vector control and veterinary services; and
- xiv. Victim identification and mortuary services.

3. NOTICE OF CONTRACT ACTION

Grantee shall notify their assigned contract manager if Grantee has had any contract suspended or terminated for cause by any local, state or federal department or agency or nonprofit entity within five days of becoming aware of the action and include the following:

- A. Reason for such action;
- B. Name and contact information of the local, state or federal department or agency or entity;
- C. Date of the contract;
- D. Date of suspension or termination; and
- E. Contract or case reference number.

4. NOTICE OF BANKRUPTCY

Grantee shall notify in writing its assigned contract manager of its plan to seek bankruptcy protection within five days of such action by Grantee.

5. CONTRACTOR NOTIFICATION OF CHANGE OF CONTACT PERSON OR KEY PERSONNEL

The Grantee shall notify in writing their contract manager assigned within ten days of any change to the Grantee's Contact Person or Key Personnel.

6. SERVICES AND INFORMATION FOR PERSONS WITH LIMITED ENGLISH PROFICIENCY

- A. Grantee shall take reasonable steps to provide services and information both orally and in writing, in appropriate languages other than English, to ensure that persons with limited English proficiency are effectively informed and can have meaningful access to programs, benefits and activities.
- B. Grantee shall identify and document on the client records the primary language/dialect of a client who has limited English proficiency and the need for translation or interpretation services and shall not require a client to provide or pay for the services of a translator or interpreter.
- C. Grantee shall make every effort to avoid use of any persons under the age of 18 or any family member or friend of the client as an interpreter for essential communications with a client with limited English proficiency, unless the client has requested that person and using the person would not compromise the effectiveness of services or violate the client's confidentiality and the client is advised that a free interpreter is available.

7. THIRD PARTY PAYORS

Except as provided in this Contract, Grantee shall screen all clients and may not bill the System Agency for services eligible for reimbursement from third party payors, who are any person or entity who has the legal responsibility for paying for all or part of the services provided, including commercial health or liability insurance carriers, Medicaid, or other federal, state, local and private funding sources.

As applicable, the Grantee shall:

- A. Enroll as a provider in Children's Health Insurance Program and Medicaid if providing approved services authorized under this Contract that may be covered by those programs and bill those programs for the covered services;
- B. Provide assistance to individuals to enroll in such programs when the screening process indicates possible eligibility for such programs;
- C. Allow clients that are otherwise eligible for System Agency services, but cannot pay a deductible required by a third-party payor, to receive services up to the amount of the deductible and to bill the System Agency for the deductible;
- D. Not bill the System Agency for any services eligible for third party reimbursement until all appeals to third party payors have been exhausted;

- E. Maintain appropriate documentation from the third-party payor reflecting attempts to obtain reimbursement;
- F. Bill all third-party payors for services provided under this Contract before submitting any request for reimbursement to System Agency; and
- G. Provide third party billing functions at no cost to the client.

8. HIV/AIDS MODEL WORKPLACE GUIDELINES

Grantee shall implement System Agency's policies based on the Human Immunodeficiency Virus/Acquired Immunodeficiency Syndrome (HIV/AIDS), AIDS Model Workplace Guidelines for Businesses at <http://www.dshs.state.tx.us/hivstd/policy/policies.shtm>, State Agencies and State Grantees Policy No. 090.021.

Grantee shall also educate employees and clients concerning HIV and its related conditions, including AIDS, in accordance with the Texas Health & Safety Code §§ 85.112-114.

9. MEDICAL RECORDS RETENTION

Grantee shall retain medical records in accordance with 22 TAC §165.1(b) or other applicable statutes, rules and regulations governing medical information.

10. NOTICE OF A LICENSE ACTION

Grantee shall notify their contract manager of any action impacting its license to provide services under this Contract within five days of becoming aware of the action and include the following:

- A. Reason for such action;
- B. Name and contact information of the local, state or federal department or agency or entity;
- C. Date of the license action; and
- D. License or case reference number.

11. INTERIM EXTENSION AMENDMENT

- A. Prior to or on the expiration date of this Contract, the Parties agree that this Contract can be extended as provided under this Section.
- B. The System Agency shall provide written notice of interim extension amendment to the Grantee under one of the following circumstances:
 - i. Continue provision of services in response to a disaster declared by the governor; or
 - ii. To ensure that services are provided to clients without interruption.
- C. The System Agency will provide written notice of the interim extension amendment that specifies the reason for it and period of time for the extension.
- D. Grantee will provide and invoice for services in the same manner that is stated in the Contract.
- E. An interim extension under Section (b)(1) above shall extend the term of the contract not longer than 30 days after governor's disaster declaration is declared unless the Parties agree to a shorter period of time.
- F. An interim extension under Section (b)(2) above shall be a one-time extension for a period of time determined by the System Agency.

**12. CONTRACTOR'S CERTIFICATION OF MEETING OR EXCEEDING TABACCO-FREE
WORKPLACE POLICY MINIMUM STANDARDS**

Grantee certifies that it has adopted and enforces a Tobacco-Free Workplace Policy that meets or exceeds all of the following minimum standards of:

- A. Prohibiting the use of all forms of tobacco products, including but not limited to cigarettes, cigars, pipes, water pipes (hookah), bidis, kreteks, electronic cigarettes, smokeless tobacco, snuff and chewing tobacco;
- B. Designating the property to which this Policy applies as a "designated area," which must at least comprise all buildings and structures where activities funded under this Contract are taking place, as well as Grantee owned, leased, or controlled sidewalks, parking lots, walkways, and attached parking structures immediately adjacent to this designated area;
- C. Applying to all employees and visitors in this designated area; and
- D. Providing for or referring its employees to tobacco use cessation services.

If Grantee cannot meet these minimum standards, it must obtain a waiver from the System Agency.

REMAINDER OF PAGE INTENTIONALLY LEFT BLANK

ASSURANCES - NON-CONSTRUCTION PROGRAMS

Public reporting burden for this collection of information is estimated to average 15 minutes per response, including time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding the burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to the Office of Management and Budget, Paperwork Reduction Project (0348-0040), Washington, DC 20503.





PLEASE DO NOT RETURN YOUR COMPLETED FORM TO THE OFFICE OF MANAGEMENT AND BUDGET. SEND IT TO THE ADDRESS PROVIDED BY THE SPONSORING AGENCY.

NOTE: Certain of these assurances may not be applicable to your project or program. If you have questions, please contact the awarding agency. Further, certain Federal awarding agencies may require applicants to certify to additional assurances. If such is the case, you will be notified.

As the duly authorized representative of the applicant, I certify that the applicant:

1. Has the legal authority to apply for Federal assistance and the institutional, managerial and financial capability (including funds sufficient to pay the non-Federal share of project cost) to ensure proper planning, management and completion of the project described in this application.
2. Will give the awarding agency, the Comptroller General of the United States and, if appropriate, the State, through any authorized representative, access to and the right to examine all records, books, papers, or documents related to the award; and will establish a proper accounting system in accordance with generally accepted accounting standards or agency directives.
3. Will establish safeguards to prohibit employees from using their positions for a purpose that constitutes or presents the appearance of personal or organizational conflict of interest, or personal gain.
4. Will initiate and complete the work within the applicable time frame after receipt of approval of the awarding agency.
5. Will comply with the Intergovernmental Personnel Act of 1970 (42 U.S.C. §§4728-4763) relating to prescribed standards for merit systems for programs funded under one of the 19 statutes or regulations specified in Appendix A of OPM's Standards for a Merit System of Personnel Administration (5 C.F.R. 900, Subpart F).
6. Will comply with all Federal statutes relating to nondiscrimination. These include but are not limited to: (a) Title VI of the Civil Rights Act of 1964 (P.L. 88-352) which prohibits discrimination on the basis of race, color or national origin; (b) Title IX of the Education Amendments of 1972, as amended (20 U.S.C. §§1681-1683, and 1685-1686), which prohibits discrimination on the basis of sex; (c) Section 504 of the Rehabilitation Act of 1973, as amended (29 U.S.C. §794), which prohibits discrimination on the basis of handicaps; (d) the Age Discrimination Act of 1975, as amended (42 U.S.C. §§6101-6107), which prohibits discrimination on the basis of age; (e) the Drug Abuse Office and Treatment Act of 1972 (P.L. 92-255), as amended, relating to nondiscrimination on the basis of drug abuse; (f) the Comprehensive Alcohol Abuse and Alcoholism Prevention, Treatment and Rehabilitation Act of 1970 (P.L. 91-616), as amended, relating to nondiscrimination on the basis of alcohol abuse or alcoholism; (g) §§523 and 527 of the Public Health Service Act of 1912 (42 U.S.C. §§290 dd-3 and 290 ee- 3), as amended, relating to confidentiality of alcohol and drug abuse patient records; (h) Title VIII of the Civil Rights Act of 1968 (42 U.S.C. §§3601 et seq.), as amended, relating to nondiscrimination in the sale, rental or financing of housing; (i) any other nondiscrimination provisions in the specific statute(s) under which application for Federal assistance is being made; and, (j) the requirements of any other nondiscrimination statute(s) which may apply to the application.
7. Will comply, or has already complied, with the requirements of Titles II and III of the Uniform Relocation Assistance and Real Property Acquisition Policies Act of 1970 (P.L. 91-646) which provide for fair and equitable treatment of persons displaced or whose property is acquired as a result of Federal or federally-assisted programs. These requirements apply to all interests in real property acquired for project purposes regardless of Federal participation in purchases.
8. Will comply, as applicable, with provisions of the Hatch Act (5 U.S.C. §§1501-1508 and 7324-7328) which limit the political activities of employees whose principal employment activities are funded in whole or in part with Federal funds.

9. Will comply, as applicable, with the provisions of the Davis-Bacon Act (40 U.S.C. §§276a to 276a-7), the Copeland Act (40 U.S.C. §276c and 18 U.S.C. §874), and the Contract Work Hours and Safety Standards Act (40 U.S.C. §§327-333), regarding labor standards for federally-assisted construction subagreements.
10. Will comply, if applicable, with flood insurance purchase requirements of Section 102(a) of the Flood Disaster Protection Act of 1973 (P.L. 93-234) which requires recipients in a special flood hazard area to participate in the program and to purchase flood insurance if the total cost of insurable construction and acquisition is \$10,000 or more.
11. Will comply with environmental standards which may be prescribed pursuant to the following: (a) institution of environmental quality control measures under the National Environmental Policy Act of 1969 (P.L. 91-190) and Executive Order (EO) 11514; (b) notification of violating facilities pursuant to EO 11738; (c) protection of wetlands pursuant to EO 11990; (d) evaluation of flood hazards in floodplains in accordance with EO 11988; (e) assurance of project consistency with the approved State management program developed under the Coastal Zone Management Act of 1972 (16 U.S.C. §§1451 et seq.); (f) conformity of Federal actions to State (Clean Air) Implementation Plans under Section 176(c) of the Clean Air Act of 1955, as amended (42 U.S.C. §§7401 et seq.); (g) protection of underground sources of drinking water under the Safe Drinking Water Act of 1974, as amended (P.L. 93-523); and, (h) protection of endangered species under the Endangered Species Act of 1973, as amended (P.L. 93-205).
12. Will comply with the Wild and Scenic Rivers Act of 1968 (16 U.S.C. §§1271 et seq.) related to protecting components or potential components of the national wild and scenic rivers system.
13. Will assist the awarding agency in assuring compliance with Section 106 of the National Historic Preservation Act of 1966, as amended (16 U.S.C. §470), EO 11593 (identification and protection of historic properties), and the Archaeological and Historic Preservation Act of 1974 (16 U.S.C. §§469a-1 et seq.).
14. Will comply with P.L. 93-348 regarding the protection of human subjects involved in research, development, and related activities supported by this award of assistance.
15. Will comply with the Laboratory Animal Welfare Act of 1966 (P.L. 89-544, as amended, 7 U.S.C. §§2131 et seq.) pertaining to the care, handling, and treatment of warm blooded animals held for research, teaching, or other activities supported by this award of assistance.
16. Will comply with the Lead-Based Paint Poisoning Prevention Act (42 U.S.C. §§4801 et seq.) which prohibits the use of lead-based paint in construction or rehabilitation of residence structures.
17. Will cause to be performed the required financial and compliance audits in accordance with the Single Audit Act Amendments of 1996 and OMB Circular No. A-133, "Audits of States, Local Governments, and Non-Profit Organizations."
18. Will comply with all applicable requirements of all other Federal laws, executive orders, regulations, and policies governing this program.
19. Will comply with the requirements of Section 106(g) of the Trafficking Victims Protection Act (TVPA) of 2000, as amended (22 U.S.C. 7104) which prohibits grant award recipients or a sub-recipient from (1) Engaging in severe forms of trafficking in persons during the period of time that the award is in effect (2) Procuring a commercial sex act during the period of time that the award is in effect or (3) Using forced labor in the performance of the award or subawards under the award.

SIGNATURE OF AUTHORIZED CERTIFYING OFFICIAL 	TITLE 
APPLICANT ORGANIZATION 	DATE SUBMITTED 

CERTIFICATION REGARDING LOBBYING

Certification for Contracts, Grants, Loans, and Cooperative Agreements

The undersigned certifies, to the best of his or her knowledge and belief, that:

(1) No Federal appropriated funds have been paid or will be paid, by or on behalf of the undersigned, to any person for influencing or attempting to influence an officer or employee of an agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with the awarding of any Federal contract, the making of any Federal grant, the making of any Federal loan, the entering into of any cooperative agreement, and the extension, continuation, renewal, amendment, or modification of any Federal contract, grant, loan, or cooperative agreement.

(2) If any funds other than Federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with this Federal contract, grant, loan, or cooperative agreement, the undersigned shall complete and submit Standard Form-LLL, "Disclosure of Lobbying Activities," in accordance with its instructions.

(3) The undersigned shall require that the language of this certification be included in the award documents for all subawards at all tiers (including subcontracts, subgrants, and contracts under grants, loans, and cooperative agreements) and that all subrecipients shall certify and disclose accordingly. This certification is a material representation of fact upon which reliance was placed when this transaction was made or entered into. Submission of this certification is a prerequisite for making or entering into this transaction imposed by section 1352, title 31, U.S. Code. Any person who fails to file the required certification shall be subject to a civil penalty of not less than \$10,000 and not more than \$100,000 for each such failure.

Statement for Loan Guarantees and Loan Insurance

The undersigned states, to the best of his or her knowledge and belief, that:

If any funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with this commitment providing for the United States to insure or guarantee a loan, the undersigned shall complete and submit Standard Form-LLL, "Disclosure of Lobbying Activities," in accordance with its instructions. Submission of this statement is a prerequisite for making or entering into this transaction imposed by section 1352, title 31, U.S. Code. Any person who fails to file the required statement shall be subject to a civil penalty of not less than \$10,000 and not more than \$100,000 for each such failure.

* APPLICANT'S ORGANIZATION <input type="text"/>	
* PRINTED NAME AND TITLE OF AUTHORIZED REPRESENTATIVE	
Prefix: <input type="text"/>	* First Name: <input type="text"/> Middle Name: <input type="text"/>
* Last Name: <input type="text"/>	Suffix: <input type="text"/>
* Title: <input type="text"/>	
* SIGNATURE: <input type="text"/>	* DATE: <input type="text"/>



Fiscal Federal Funding Accountability and Transparency Act (FFATA)

The certifications enumerated below represent material facts upon which DSHS relies when reporting information to the federal government required under federal law. If the Department later determines that the Contractor knowingly rendered an erroneous certification, DSHS may pursue all available remedies in accordance with Texas and U.S. law. Signor further agrees that it will provide immediate written notice to DSHS if at any time Signor learns that any of the certifications provided for below were erroneous when submitted or have since become erroneous by reason of changed circumstances. ***If the Signor cannot certify all of the statements contained in this section, Signor must provide written notice to DSHS detailing which of the below statements it cannot certify and why.***

Legal Name of Contractor:	FFATA Contact: (Name, Email and Phone Number):
Primary Address of Contractor:	Zip Code: 9-digits required www.usps.com
Unique Entity ID (UEI): This number replaces the DUNS www.sam.gov	State of Texas Comptroller Vendor Identification Number (VIN) – 14 digits:

Printed Name of Authorized Representative:	Signature of Authorized Representative
Title of Authorized Representative	Date Signed

Fiscal Federal Funding Accountability and Transparency Act (FFATA) CERTIFICATION

As the duly authorized representative (Signor) of the Contractor, I hereby certify that the statements made by me in this certification form are true, complete, and correct to the best of my knowledge.

Did your organization have a gross income, from all sources, of less than \$300,000 in your previous tax year? Yes No

If your answer is "Yes", skip questions "A", "B", and "C" and finish the certification. If your answer is "No", answer questions "A" and "B".

A. Certification Regarding % of Annual Gross from Federal Awards.

Did your organization receive 80% or more of its annual gross revenue from federal awards during the preceding fiscal year? Yes No

B. Certification Regarding Amount of Annual Gross from Federal Awards.

Did your organization receive \$25 million or more in annual gross revenues from federal awards in the preceding fiscal year? Yes No

If your answer is "Yes" to both question "A" and "B", you must answer question "C".
If your answer is "No" to either question "A" or "B", skip question "C" and finish the certification.

C. Certification Regarding Public Access to Compensation Information.

Does the public have access to information about the compensation of the senior executives in your business or organization (including parent organization, all branches, and all affiliates worldwide) through periodic reports filed under section 13(a) or 15(d) of the Securities Exchange Act of 1934 (15 U.S.C. 78m(a), 78o(d)) or section 6104 of the Internal Revenue Code of 1986? Yes No

If your answer is "Yes" to this question, where can this information be accessed?

If your answer is "No" to this question, you must provide the names and total compensation of the top five highly compensated officers below.

Provide compensation information here:

HHS DATA USE AGREEMENT

This Data Use Agreement (“DUA”), effective as of the date the Base Contract into which it is incorporated is signed (“Effective Date”), is entered into by and between a Texas Health and Human Services Enterprise agency (“HHS”), and the Contractor identified in the Base Contract, a political subdivision of the State of Texas (“CONTRACTOR”).

ARTICLE 1.

PURPOSE; APPLICABILITY; ORDER OF PRECEDENCE

The purpose of this DUA is to facilitate creation, receipt, maintenance, use, disclosure or access to Confidential Information with CONTRACTOR, and describe CONTRACTOR’s rights and obligations with respect to the Confidential Information. **45 CFR 164.504(e)(1)-(3)**. This DUA also describes HHS’s remedies in the event of CONTRACTOR’s noncompliance with its obligations under this DUA. This DUA applies to both Business Associates and contractors who are not Business Associates who create, receive, maintain, use, disclose or have access to Confidential Information on behalf of HHS, its programs or clients as described in the Base Contract.

As of the Effective Date of this DUA, if any provision of the Base Contract, including any General Provisions or Uniform Terms and Conditions, conflicts with this DUA, this DUA controls.

ARTICLE 2.

DEFINITIONS

For the purposes of this DUA, capitalized, underlined terms have the meanings set forth in the following: Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 (42 U.S.C. §1320d, *et seq.*) and regulations thereunder in 45 CFR Parts 160 and 164, including all amendments, regulations and guidance issued thereafter; The Social Security Act, including Section 1137 (42 U.S.C. §§ 1320b-7), Title XVI of the Act; The Privacy Act of 1974, as amended by the Computer Matching and Privacy Protection Act of 1988, 5 U.S.C. § 552a and regulations and guidance thereunder; Internal Revenue Code, Title 26 of the United States Code and regulations and publications adopted under that code, including IRS Publication 1075; OMB Memorandum 07-18; Texas Business and Commerce Code Ch. 521; Texas Government Code, Ch. 552, and Texas Government Code §2054.1125. In addition, the following terms in this DUA are defined as follows:

“**Authorized Purpose**” means the specific purpose or purposes described in the Statement of Work of the Base Contract for CONTRACTOR to fulfill its obligations under the Base Contract, or any other purpose expressly authorized by HHS in writing in advance.

“**Authorized User**” means a Person:

(1) Who is authorized to create, receive, maintain, have access to, process, view, handle, examine, interpret, or analyze Confidential Information pursuant to this DUA;

(2) For whom CONTRACTOR warrants and represents has a demonstrable need to create, receive, maintain, use, disclose or have access to the Confidential Information; and

(3) Who has agreed in writing to be bound by the disclosure and use limitations pertaining to the Confidential Information as required by this DUA.

“Confidential Information” means any communication or record (whether oral, written, electronically stored or transmitted, or in any other form) provided to or made available to CONTRACTOR, or that CONTRACTOR may, for an Authorized Purpose, create, receive, maintain, use, disclose or have access to, that consists of or includes any or all of the following:

- (1) Client Information;
- (2) Protected Health Information in any form including without limitation, Electronic Protected Health Information or Unsecured Protected Health Information (herein “PHI”);
- (3) Sensitive Personal Information defined by Texas Business and Commerce Code Ch. 521;
- (4) Federal Tax Information;
- (5) Individually Identifiable Health Information as related to HIPAA, Texas HIPAA and Personal Identifying Information under the Texas Identity Theft Enforcement and Protection Act;
- (6) Social Security Administration Data, including, without limitation, Medicaid information;
- (7) All privileged work product;
- (8) All information designated as confidential under the constitution and laws of the State of Texas and of the United States, including the Texas Health & Safety Code and the Texas Public Information Act, Texas Government Code, Chapter 552.

“Legally Authorized Representative” of the Individual, as defined by Texas law, including as provided in 45 CFR 435.923 (Medicaid); 45 CFR 164.502(g)(1) (HIPAA); Tex. Occ. Code § 151.002(6); Tex. H. & S. Code §166.164; and Estates Code Ch. 752.

ARTICLE 3.

CONTRACTOR'S DUTIES REGARDING CONFIDENTIAL INFORMATION

3.01 Obligations of CONTRACTOR

CONTRACTOR agrees that:

(A) CONTRACTOR will exercise reasonable care and no less than the same degree of care CONTRACTOR uses to protect its own confidential, proprietary and trade secret information to prevent any portion of the Confidential Information from being used in

HHS Data Use Agreement

TACCHO VERSION (Local City and County Entities) **October 23**, 2019

a manner that is not expressly an Authorized Purpose under this DUA or as Required by Law. **45 CFR 164.502(b)(1); 45 CFR 164.514(d)**

(B) Except as Required by Law, CONTRACTOR will not disclose or allow access to any portion of the Confidential Information to any Person or other entity, other than Authorized User's Workforce or Subcontractors (as defined in **45 C.F.R. 160.103**) of CONTRACTOR who have completed training in confidentiality, privacy, security and the importance of promptly reporting any Event or Breach to CONTRACTOR's management, to carry out CONTRACTOR's obligations in connection with the Authorized Purpose.

HHS, at its election, may assist CONTRACTOR in training and education on specific or unique HHS processes, systems and/or requirements. CONTRACTOR will produce evidence of completed training to HHS upon request. **45 C.F.R. 164.308(a)(5)(i); Texas Health & Safety Code §181.101**

All of CONTRACTOR's Authorized Users, Workforce and Subcontractors with access to a state computer system or database will complete a cybersecurity training program certified under Texas Government Code Section 2054.519 by the Texas Department of Information Resources or offered under Texas Government Code Sec. 2054.519(f).

(C) CONTRACTOR will establish, implement and maintain appropriate sanctions against any member of its Workforce or Subcontractor who fails to comply with this DUA, the Base Contract or applicable law. CONTRACTOR will maintain evidence of sanctions and produce it to HHS upon request. **45 C.F.R. 164.308(a)(1)(ii)(C); 164.530(e); 164.410(b); 164.530(b)(1)**

(D) CONTRACTOR will not, except as otherwise permitted by this DUA, disclose or provide access to any Confidential Information on the basis that such act is Required by Law without notifying either HHS or CONTRACTOR's own legal counsel to determine whether CONTRACTOR should object to the disclosure or access and seek appropriate relief. CONTRACTOR will maintain an accounting of all such requests for disclosure and responses and provide such accounting to HHS within 48 hours of HHS' request. **45 CFR 164.504(e)(2)(ii)(A)**

(E) CONTRACTOR will not attempt to re-identify or further identify Confidential Information or De-identified Information, or attempt to contact any Individuals whose records are contained in the Confidential Information, except for an Authorized Purpose, without express written authorization from HHS or as expressly permitted by the Base Contract. **45 CFR 164.502(d)(2)(i) and (ii)** CONTRACTOR will not engage in prohibited marketing or sale of Confidential Information. **45 CFR 164.501, 164.508(a)(3) and (4); Texas Health & Safety Code Ch. 181.002**

(F) CONTRACTOR will not permit, or enter into any agreement with a Subcontractor to, create, receive, maintain, use, disclose, have access to or transmit Confidential Information to carry out CONTRACTOR's obligations in connection with the Authorized Purpose on behalf of CONTRACTOR, unless Subcontractor agrees to comply

with all applicable laws, rules and regulations. **45 CFR 164.502(e)(1)(ii); 164.504(e)(1)(i) and (2).**

(G) CONTRACTOR is directly responsible for compliance with, and enforcement of, all conditions for creation, maintenance, use, disclosure, transmission and Destruction of Confidential Information and the acts or omissions of Subcontractors as may be reasonably necessary to prevent unauthorized use. **45 CFR 164.504(e)(5); 42 CFR 431.300, et seq.**

(H) If CONTRACTOR maintains PHI in a Designated Record Set which is Confidential Information and subject to this Agreement, CONTRACTOR will make PHI available to HHS in a Designated Record Set upon request. CONTRACTOR will provide PHI to an Individual, or Legally Authorized Representative of the Individual who is requesting PHI in compliance with the requirements of the HIPAA Privacy Regulations. CONTRACTOR will release PHI in accordance with the HIPAA Privacy Regulations upon receipt of a valid written authorization. CONTRACTOR will make other Confidential Information in CONTRACTOR's possession available pursuant to the requirements of HIPAA or other applicable law upon a determination of a Breach of Unsecured PHI as defined in HIPAA. CONTRACTOR will maintain an accounting of all such disclosures and provide it to HHS within 48 hours of HHS' request. **45 CFR 164.524 and 164.504(e)(2)(ii)(E).**

(I) If PHI is subject to this Agreement, CONTRACTOR will make PHI as required by HIPAA available to HHS for review subsequent to CONTRACTOR's incorporation of any amendments requested pursuant to HIPAA. **45 CFR 164.504(e)(2)(ii)(E) and (F).**

(J) If PHI is subject to this Agreement, CONTRACTOR will document and make available to HHS the PHI required to provide access, an accounting of disclosures or amendment in compliance with the requirements of the HIPAA Privacy Regulations. **45 CFR 164.504(e)(2)(ii)(G) and 164.528.**

(K) If CONTRACTOR receives a request for access, amendment or accounting of PHI from an individual with a right of access to information subject to this DUA, it will respond to such request in compliance with the HIPAA Privacy Regulations. CONTRACTOR will maintain an accounting of all responses to requests for access to or amendment of PHI and provide it to HHS within 48 hours of HHS' request. **45 CFR 164.504(e)(2).**

(L) CONTRACTOR will provide, and will cause its Subcontractors and agents to provide, to HHS periodic written certifications of compliance with controls and provisions relating to information privacy, security and breach notification, including without limitation information related to data transfers and the handling and disposal of Confidential Information. **45 CFR 164.308; 164.530(c); 1 TAC 202.**

(M) Except as otherwise limited by this DUA, the Base Contract, or law applicable to the Confidential Information, CONTRACTOR may use PHI for the proper management and administration of CONTRACTOR or to carry out CONTRACTOR's

legal responsibilities. Except as otherwise limited by this DUA, the Base Contract, or law applicable to the Confidential Information, CONTRACTOR may disclose PHI for the proper management and administration of CONTRACTOR, or to carry out CONTRACTOR's legal responsibilities, if: **45 CFR 164.504(e)(4)(A)**.

(1) Disclosure is Required by Law, provided that CONTRACTOR complies with Section 3.01(D); or

(2) CONTRACTOR obtains reasonable assurances from the person or entity to which the information is disclosed that the person or entity will:

(a) Maintain the confidentiality of the Confidential Information in accordance with this DUA;

(b) Use or further disclose the information only as Required by Law or for the Authorized Purpose for which it was disclosed to the Person; and

(c) Notify CONTRACTOR in accordance with Section 4.01 of any Event or Breach of Confidential Information of which the Person discovers or should have discovered with the exercise of reasonable diligence. **45 CFR 164.504(e)(4)(ii)(B)**.

(N) Except as otherwise limited by this DUA, CONTRACTOR will, if required by law and requested by HHS, use commercially reasonable efforts to use PHI to provide data aggregation services to HHS, as that term is defined in the HIPAA, 45 C.F.R. §164.501 and permitted by HIPAA. **45 CFR 164.504(e)(2)(i)(B)**

(O) CONTRACTOR will, on the termination or expiration of this DUA or the Base Contract, at its expense, send to HHS or Destroy, at HHS's election and to the extent reasonably feasible and permissible by law, all Confidential Information received from HHS or created or maintained by CONTRACTOR or any of CONTRACTOR's agents or Subcontractors on HHS's behalf if that data contains Confidential Information. CONTRACTOR will certify in writing to HHS that all the Confidential Information that has been created, received, maintained, used by or disclosed to CONTRACTOR, has been Destroyed or sent to HHS, and that CONTRACTOR and its agents and Subcontractors have retained no copies thereof. Notwithstanding the foregoing, HHS acknowledges and agrees that CONTRACTOR is not obligated to send to HHSC and/or Destroy any Confidential Information if federal law, state law, the Texas State Library and Archives Commission records retention schedule, and/or a litigation hold notice prohibit such delivery or Destruction. If such delivery or Destruction is not reasonably feasible, or is impermissible by law, CONTRACTOR will immediately notify HHS of the reasons such delivery or Destruction is not feasible, and agree to extend indefinitely the protections of this DUA to the Confidential Information and limit its further uses and disclosures to the purposes that make the return delivery or Destruction of the Confidential Information not feasible for as long as CONTRACTOR maintains such Confidential Information. **45 CFR 164.504(e)(2)(ii)(J)**

(P) CONTRACTOR will create, maintain, use, disclose, transmit or Destroy Confidential Information in a secure fashion that protects against any reasonably anticipated threats or hazards to the security or integrity of such information or unauthorized uses. **45 CFR 164.306; 164.530(c)**

(Q) If CONTRACTOR accesses, transmits, stores, and/or maintains Confidential Information, CONTRACTOR will complete and return to HHS at infosecurity@hhsc.state.tx.us the HHS information security and privacy initial inquiry (SPI) at Attachment 1 . The SPI identifies basic privacy and security controls with which CONTRACTOR must comply to protect HHS Confidential Information. CONTRACTOR will comply with periodic security controls compliance assessment and monitoring by HHS as required by state and federal law, based on the type of Confidential Information CONTRACTOR creates, receives, maintains, uses, discloses or has access to and the Authorized Purpose and level of risk. CONTRACTOR's security controls will be based on the National Institute of Standards and Technology (NIST) Special Publication 800-53. CONTRACTOR will update its security controls assessment whenever there are significant changes in security controls for HHS Confidential Information and will provide the updated document to HHS. HHS also reserves the right to request updates as needed to satisfy state and federal monitoring requirements. **45 CFR 164.306.**

(R) CONTRACTOR will establish, implement and maintain reasonable procedural, administrative, physical and technical safeguards to preserve and maintain the confidentiality, integrity, and availability of the Confidential Information, and with respect to PHI, as described in the HIPAA Privacy and Security Regulations, or other applicable laws or regulations relating to Confidential Information, to prevent any unauthorized use or disclosure of Confidential Information as long as CONTRACTOR has such Confidential Information in its actual or constructive possession. **45 CFR 164.308 (administrative safeguards); 164.310 (physical safeguards); 164.312 (technical safeguards); 164.530(c)(privacy safeguards).**

(S) CONTRACTOR will designate and identify, a Person or Persons, as Privacy Official **45 CFR 164.530(a)(1)** and Information Security Official, each of whom is authorized to act on behalf of CONTRACTOR and is responsible for the development and implementation of the privacy and security requirements in this DUA. CONTRACTOR will provide name and current address, phone number and e-mail address for such designated officials to HHS upon execution of this DUA and prior to any change. If such persons fail to develop and implement the requirements of the DUA, CONTRACTOR will replace them upon HHS request. **45 CFR 164.308(a)(2).**

(T) CONTRACTOR represents and warrants that its Authorized Users each have a demonstrated need to know and have access to Confidential Information solely to the minimum extent necessary to accomplish the Authorized Purpose pursuant to this DUA and the Base Contract, and further, that each has agreed in writing to be bound by the disclosure and use limitations pertaining to the Confidential Information contained in this DUA. **45 CFR 164.502; 164.514(d).**

(U) CONTRACTOR and its Subcontractors will maintain an updated, complete, accurate and numbered list of Authorized Users, their signatures, titles and the date they agreed to be bound by the terms of this DUA, at all times and supply it to HHS, as directed, upon request.

(V) CONTRACTOR will implement, update as necessary, and document reasonable and appropriate policies and procedures for privacy, security and Breach of Confidential Information and an incident response plan for an Event or Breach, to comply with the privacy, security and breach notice requirements of this DUA prior to conducting work under the Statement of Work. **45 CFR 164.308; 164.316; 164.514(d); 164.530(i)(1).**

(W) CONTRACTOR will produce copies of its information security and privacy policies and procedures and records relating to the use or disclosure of Confidential Information received from, created by, or received, used or disclosed by CONTRACTOR for an Authorized Purpose for HHS's review and approval within 30 days of execution of this DUA and upon request by HHS the following business day or other agreed upon time frame. **45 CFR 164.308; 164.514(d).**

(X) CONTRACTOR will make available to HHS any information HHS requires to fulfill HHS's obligations to provide access to, or copies of, PHI in accordance with HIPAA and other applicable laws and regulations relating to Confidential Information. CONTRACTOR will provide such information in a time and manner reasonably agreed upon or as designated by the Secretary of the U.S. Department of Health and Human Services, or other federal or state law. **45 CFR 164.504(e)(2)(i)(I).**

(Y) CONTRACTOR will only conduct secure transmissions of Confidential Information whether in paper, oral or electronic form, in accordance with applicable rules, regulations and laws. A secure transmission of electronic Confidential Information in motion includes, but is not limited to, Secure File Transfer Protocol (SFTP) or Encryption at an appropriate level. If required by rule, regulation or law, HHS Confidential Information at rest requires Encryption unless there is other adequate administrative, technical, and physical security. All electronic data transfer and communications of Confidential Information will be through secure systems. Proof of system, media or device security and/or Encryption must be produced to HHS no later than 48 hours after HHS's written request in response to a compliance investigation, audit or the Discovery of an Event or Breach. Otherwise, requested production of such proof will be made as agreed upon by the parties. De-identification of HHS Confidential Information is a means of security. With respect to de-identification of PHI, "secure" means de-identified according to HIPAA Privacy standards and regulatory guidance. **45 CFR 164.312; 164.530(d).**

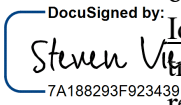
(Z) For each type of Confidential Information CONTRACTOR creates, receives, maintains, uses, discloses, has access to or transmits in the performance of the Statement of Work, CONTRACTOR will comply with the following laws rules and regulations, only to the extent applicable and required by law:

- Title 1, Part 10, Chapter 202, Subchapter B, Texas Administrative Code;

- The Privacy Act of 1974;
- OMB Memorandum 07-16;
- The Federal Information Security Management Act of 2002 (FISMA);
- The Health Insurance Portability and Accountability Act of 1996 (HIPAA) as defined in the DUA;
- Internal Revenue Publication 1075 – Tax Information Security Guidelines for Federal, State and Local Agencies;
- National Institute of Standards and Technology (NIST) Special Publication 800-66 Revision 1 – An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule;
- NIST Special Publications 800-53 and 800-53A – Recommended Security Controls for Federal Information Systems and Organizations, as currently revised;
- NIST Special Publication 800-47 – Security Guide for Interconnecting Information Technology Systems;
- NIST Special Publication 800-88, Guidelines for Media Sanitization;
- NIST Special Publication 800-111, Guide to Storage of Encryption Technologies for End User Devices containing PHI; and

Any other State or Federal law, regulation, or administrative rule relating to the specific HHS program area that CONTRACTOR supports on behalf of HHS.

(AA) Notwithstanding anything to the contrary herein, CONTRACTOR will treat any Personal Identifying Information it creates, receives, maintains, uses, transmits, destroys and/or discloses in accordance with Texas Business and Commerce Code, Chapter 521 and other applicable regulatory standards identified in Section 3.01(Z), and Individually Identifiable Health Information CONTRACTOR creates, receives, maintains, uses, transmits, destroys and/or discloses in accordance with HIPAA and other applicable regulatory standards identified in Section 3.01(Z).

DocuSigned by:

 Steven Vira
 7A188293F923439

May 16, 2022

na

ARTICLE 4.
BREACH NOTICE, REPORTING AND CORRECTION REQUIREMENTS

4.01 Breach or Event Notification to HHS. 45 CFR 164.400-414.

(A) CONTRACTOR will cooperate fully with HHS in investigating, mitigating to the extent practicable and issuing notifications directed by HHS, for any Event or Breach of Confidential Information to the extent and in the manner determined by HHS.

(B) CONTRACTOR'S obligation begins at the Discovery of an Event or Breach and continues as long as related activity continues, until all effects of the Event are mitigated to HHS's reasonable satisfaction (the "incident response period"). **45 CFR 164.404.**

(C) Breach Notice:

(1) Initial Notice.

(a) For federal information, including without limitation, Federal Tax Information, Social Security Administration Data, and Medicaid Client Information, within the first, consecutive clock hour of Discovery, and for all other types of Confidential Information not more than 24 hours after Discovery, or in a timeframe otherwise approved by HHS in writing, initially report to HHS's Privacy and Security Officers via email at: privacy@HHSC.state.tx.us and to the HHS division responsible for this DUA; and IRS Publication 1075; Privacy Act of 1974, as amended by the Computer Matching and Privacy Protection Act of 1988, 5 U.S.C. § 552a; OMB Memorandum 07-16 as cited in HHSC-CMS Contracts for information exchange.

(b) Report all information reasonably available to CONTRACTOR about the Event or Breach of the privacy or security of Confidential Information. **45 CFR 164.410.**

(c) Name, and provide contact information to HHS for, CONTRACTOR's single point of contact who will communicate with HHS both on and off business hours during the incident response period.

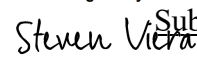
na (2) Formal Notice. No later than two business days after the Initial Notice above, provide formal notification to privacy@HHSC.state.tx.us and to the HHS division responsible for this DUA, including all reasonably available information about the Event or Breach, and CONTRACTOR's investigation, including without limitation and to the extent available: **For (a) - (m) below: 45 CFR 164.400-414.**

na

na

(a) The date the Event or Breach occurred;

(b) The date of CONTRACTOR's, and, if applicable, Subcontractor's Discovery;

DocuSigned by:

7A188293F923439...

(c) A brief description of the Event or Breach; including how it occurred and who is responsible (or hypotheses, if not yet determined);

(d) A brief description of CONTRACTOR's investigation and the status of the investigation;

(e) A description of the types and amount of Confidential Information involved;

(f) Identification of and number of all Individuals reasonably believed to be affected, including first and last name of the Individual and if applicable the, Legally Authorized Representative, last known address, age, telephone number, and email address if it is a preferred contact method, to the extent known or can be reasonably determined by CONTRACTOR at that time;

na (g) CONTRACTOR's initial risk assessment of the Event or Breach demonstrating whether individual or other notices are required by applicable law or this DUA for HHS approval, including an analysis of whether there is a low probability of compromise of the Confidential Information or whether any legal exceptions to notification apply;

na (h) CONTRACTOR's recommendation for HHS's approval as to the steps Individuals and/or CONTRACTOR on behalf of Individuals, should take to protect the Individuals from potential harm, including without limitation CONTRACTOR's provision of notifications, credit protection, claims monitoring, and any specific protections for a Legally Authorized Representative to take on behalf of an Individual with special capacity or circumstances;

na (i) The steps CONTRACTOR has taken to mitigate the harm or potential harm caused (including without limitation the provision of sufficient resources to mitigate);

na (j) The steps CONTRACTOR has taken, or will take, to prevent or reduce the likelihood of recurrence of a similar Event or Breach;

(k) Identify, describe or estimate the Persons, Workforce, Subcontractor, or Individuals and any law enforcement that may be involved in the Event or Breach;

na (l) A reasonable schedule for CONTRACTOR to provide regular updates during normal business hours to the foregoing in the future for response to the Event or Breach, but no less than every three (3) business days or as otherwise directed by HHS, including information about risk estimations, reporting, notification, if any, mitigation, corrective action, root cause analysis and when such activities are expected to be completed; and
DocuSigned by:
Steven Vera
7A186293-F229-4381-8000-000000000000
May 16, 2022

(m) Any reasonably available, pertinent information, documents or reports related to an Event or Breach that HHS requests following Discovery.

4.02 Investigation, Response and Mitigation. 45 CFR 164.308, 310 and 312; 164.530

(A) CONTRACTOR will immediately conduct a full and complete investigation, respond to the Event or Breach, commit necessary and appropriate staff and resources to expeditiously respond, and report as required to and by HHS for incident response purposes and for purposes of HHS's compliance with report and notification requirements, to the reasonable satisfaction of HHS.

(B) CONTRACTOR will complete or participate in a risk assessment as directed by HHS following an Event or Breach, and provide the final assessment, corrective actions and mitigations to HHS for review and approval.

(C) CONTRACTOR will fully cooperate with HHS to respond to inquiries and/or proceedings by state and federal authorities, Persons and/or Individuals about the Event or Breach.

(D) CONTRACTOR will fully cooperate with HHS's efforts to seek appropriate injunctive relief or otherwise prevent or curtail such Event or Breach, or to recover or protect any Confidential Information, including complying with reasonable corrective action or measures, as specified by HHS in a Corrective Action Plan if directed by HHS under the Base Contract.

4.03 Breach Notification to Individuals and Reporting to Authorities. Tex. Bus. & Comm. Code §521.053; 45 CFR 164.404 (Individuals), 164.406 (Media); 164.408 (Authorities)

(A) HHS may direct CONTRACTOR to provide Breach notification to Individuals, regulators or third-parties, as specified by HHS following a Breach.

(B) CONTRACTOR shall give HHS an opportunity to review and provide feedback to CONTRACTOR and to confirm that CONTRACTOR's notice meets all regulatory requirements regarding the time, manner and content of any notification to Individuals, regulators or third-parties, or any notice required by other state or federal authorities, **including without limitation, notifications required by Texas Business and Commerce Code, Chapter 521.053(b) and HIPAA**. HHS shall have ten (10) business days to provide said feedback to CONTRACTOR. Notice letters will be in CONTRACTOR's name and on CONTRACTOR's letterhead, unless otherwise directed by HHS, and will contain contact information, including the name and title of CONTRACTOR's representative, an email address and a toll-free telephone number, if required by applicable law, rule, or regulation, for the Individual to obtain additional information.

(C) CONTRACTOR will provide HHS with copies of distributed and approved communications.

(D) CONTRACTOR will have the burden of demonstrating to the reasonable satisfaction of HHS that any notification required by HHS was timely made. If there are delays outside of CONTRACTOR's control, CONTRACTOR will provide written documentation of the reasons for the delay.

(E) If HHS delegates notice requirements to CONTRACTOR, HHS shall, in the time and manner reasonably requested by CONTRACTOR, cooperate and assist with CONTRACTOR's information requests in order to make such notifications and reports.

ARTICLE 5. STATEMENT OF WORK

“Statement of Work” means the services and deliverables to be performed or provided by CONTRACTOR, or on behalf of CONTRACTOR by its Subcontractors or agents for HHS that are described in detail in the Base Contract. The Statement of Work, including any future amendments thereto, is incorporated by reference in this DUA as if set out word-for-word herein.

ARTICLE 6. GENERAL PROVISIONS

6.01 Oversight of Confidential Information

CONTRACTOR acknowledges and agrees that HHS is entitled to oversee and monitor CONTRACTOR's access to and creation, receipt, maintenance, use, disclosure of the Confidential Information to confirm that CONTRACTOR is in compliance with this DUA.

6.02 HHS Commitment and Obligations

HHS will not request CONTRACTOR to create, maintain, transmit, use or disclose PHI in any manner that would not be permissible under applicable law if done by HHS.

6.03 HHS Right to Inspection

At any time upon reasonable notice to CONTRACTOR, or if HHS determines that CONTRACTOR has violated this DUA, HHS, directly or through its agent, will have the right to inspect the facilities, systems, books and records of CONTRACTOR to monitor compliance with this DUA. For purposes of this subsection, HHS's agent(s) include, without limitation, the HHS Office of the Inspector General or the Office of the Attorney General of Texas, outside consultants or legal counsel or other designee.

6.04 Term; Termination of DUA; Survival

This DUA will be effective on the date on which CONTRACTOR executes the DUA, and will terminate upon termination of the Base Contract and as set forth herein. If the Base Contract is extended or amended, this DUA shall be extended or amended concurrent with such extension or amendment.

(A) HHS may immediately terminate this DUA and Base Contract upon a material violation of this DUA.

(B) Termination or Expiration of this DUA will not relieve CONTRACTOR of its obligation to return or Destroy the Confidential Information as set forth in this DUA and to continue to safeguard the Confidential Information until such time as determined by HHS.

(C) If HHS determines that CONTRACTOR has violated a material term of this DUA; HHS may in its sole discretion:

(1) Exercise any of its rights including but not limited to reports, access and inspection under this DUA and/or the Base Contract; or

(2) Require CONTRACTOR to submit to a Corrective Action Plan, including a plan for monitoring and plan for reporting, as HHS may determine necessary to maintain compliance with this DUA; or

(3) Provide CONTRACTOR with a reasonable period to cure the violation as determined by HHS; or

(4) Terminate the DUA and Base Contract immediately, and seek relief in a court of competent jurisdiction in Texas.

Before exercising any of these options, HHS will provide written notice to CONTRACTOR describing the violation, the requested corrective action CONTRACTOR may take to cure the alleged violation, and the action HHS intends to take if the alleged violated is not timely cured by CONTRACTOR.

(D) If neither termination nor cure is feasible, HHS shall report the violation to the Secretary of the U.S. Department of Health and Human Services.

(E) The duties of CONTRACTOR or its Subcontractor under this DUA survive the expiration or termination of this DUA until all the Confidential Information is Destroyed or returned to HHS, as required by this DUA.

6.05 Governing Law, Venue and Litigation

(A) The validity, construction and performance of this DUA and the legal relations among the Parties to this DUA will be governed by and construed in accordance with the laws of the State of Texas.

(B) The Parties agree that the courts of Texas, will be the exclusive venue for any litigation, special proceeding or other proceeding as between the parties that may be brought, or arise out of, or in connection with, or by reason of this DUA.

6.06 Injunctive Relief

(A) CONTRACTOR acknowledges and agrees that HHS may suffer irreparable injury if CONTRACTOR or its Subcontractor fails to comply with any of the terms of this DUA with respect to the Confidential Information or a provision of HIPAA or other laws or regulations applicable to Confidential Information.

(B) CONTRACTOR further agrees that monetary damages may be inadequate to compensate HHS for CONTRACTOR's or its Subcontractor's failure to comply. Accordingly, CONTRACTOR agrees that HHS will, in addition to any other remedies available to it at law or in equity, be entitled to seek injunctive relief without posting a bond and without the necessity of demonstrating actual damages, to enforce the terms of this DUA.

6.07 Responsibility.

To the extent permitted by the Texas Constitution, laws and rules, and without waiving any immunities or defenses available to CONTRACTOR as a governmental entity, CONTRACTOR shall be solely responsible for its own acts and omissions and the acts and omissions of its employees, directors, officers, Subcontractors and agents. HHS shall be solely responsible for its own acts and omissions.

6.08 Insurance

(A) As a governmental entity, and in accordance with the limits of the Texas Tort Claims Act, Chapter 101 of the Texas Civil Practice and Remedies Code, CONTRACTOR either maintains commercial insurance or self-insures with policy limits in an amount sufficient to cover CONTRACTOR's liability arising under this DUA. CONTRACTOR will request that HHS be named as an additional insured. HHS reserves the right to consider alternative means for CONTRACTOR to satisfy CONTRACTOR's financial responsibility under this DUA. Nothing herein shall relieve CONTRACTOR of its financial obligations set forth in this DUA if CONTRACTOR fails to maintain insurance.

(B) CONTRACTOR will provide HHS with written proof that required insurance coverage is in effect, at the request of HHS.

6.08 Fees and Costs

Except as otherwise specified in this DUA or the Base Contract, if any legal action or other proceeding is brought for the enforcement of this DUA, or because of an alleged dispute, contract violation, Event, Breach, default, misrepresentation, or injunctive action, in connection with any of the provisions of this DUA, each party will bear their own legal expenses and the other cost incurred in that action or proceeding.

6.09 Entirety of the Contract

This DUA is incorporated by reference into the Base Contract as an amendment thereto and, together with the Base Contract, constitutes the entire agreement between the parties. No change, waiver, or discharge of obligations arising under those documents will be valid unless in writing and executed by the party against whom such change, waiver, or discharge is sought to be

enforced. If any provision of the Base Contract, including any General Provisions or Uniform Terms and Conditions, conflicts with this DUA, this DUA controls.

6.10 Automatic Amendment and Interpretation

If there is (i) a change in any law, regulation or rule, state or federal, applicable to HIPPA and/or Confidential Information, or (ii) any change in the judicial or administrative interpretation of any such law, regulation or rule,, upon the effective date of such change, this DUA shall be deemed to have been automatically amended, interpreted and read so that the obligations imposed on HHS and/or CONTRACTOR remain in compliance with such changes. Any ambiguity in this DUA will be resolved in favor of a meaning that permits HHS and CONTRACTOR to comply with HIPAA or any other law applicable to Confidential Information.



**Texas HHS System - Data Use Agreement - Attachment 2
SECURITY AND PRIVACY INQUIRY (SPI)**

If you are a bidder for a new procurement/contract, in order to participate in the bidding process, you must have corrected any "No" responses (except A9a) prior to the contract award date. If you are an applicant for an open enrollment, you must have corrected any "No" answers (except A9a and A11) prior to performing any work on behalf of any Texas HHS agency.

For any questions answered "No" (except A9a and A11), an *Action Plan for Compliance with a Timeline* must be documented in the designated area below the question. The timeline for compliance with HIPAA-related requirements for safeguarding Protected Health Information is 30 calendar days from the date this form is signed. Compliance with requirements related to other types of Confidential Information must be confirmed within 90 calendar days from the date the form is signed.

SECTION A: APPLICANT/BIDDER INFORMATION (To be completed by Applicant/Bidder)

<p>1. Does the applicant/bidder access, create, disclose, receive, transmit, maintain, or store Texas HHS Confidential Information in electronic systems (e.g., laptop, personal use computer, mobile device, database, server, etc.)? IF NO, STOP. THE SPI FORM IS NOT REQUIRED.</p>	<p align="right"> <input type="radio"/> Yes <input type="radio"/> No </p>
<p>2. Entity or Applicant/Bidder Legal Name</p>	<p>Legal Name: Legal Entity Tax Identification Number (TIN) (Last Four Numbers Only): Procurement/Contract#: Address: City: State: ZIP: Telephone #: Email Address:</p>
<p>3. Number of Employees, at all locations, in Applicant/Bidder's Workforce "Workforce" means all employees, volunteers, trainees, and other Persons whose conduct is under the direct control of Applicant/Bidder, whether or not they are paid by Applicant/Bidder. If Applicant/Bidder is a sole proprietor, the workforce may be only one employee.</p>	<p>Total Employees:</p>
<p>4. Number of Subcontractors (if Applicant/Bidder will not use subcontractors, enter "0")</p>	<p>Total Subcontractors:</p>
<p>5. Name of Information Technology Security Official and Name of Privacy Official for Applicant/Bidder (Privacy and Security Official may be the same person.)</p>	<p>A. Security Official: Legal Name: Address: City: State: ZIP: Telephone #: Email Address:</p> <hr/> <p>B. Privacy Official: Legal Name: Address: City: State: ZIP: Telephone #: Email Address:</p>

6. Type(s) of Texas HHS Confidential Information the Applicant/Bidder will create, receive, maintain, use, disclose or have access to: (Check all that apply)

- Health Insurance Portability and Accountability Act (HIPAA) data
- Criminal Justice Information Services (CJIS) data
- Internal Revenue Service Federal Tax Information (IRS FTI) data
- Centers for Medicare & Medicaid Services (CMS)
- Social Security Administration (SSA)
- Personally Identifiable Information (PII)

HIPAA <input type="checkbox"/>	CJIS <input type="checkbox"/>	IRS FTI <input type="checkbox"/>	CMS <input type="checkbox"/>	SSA <input type="checkbox"/>	PII <input type="checkbox"/>
Other (Please List)					

7. Number of Storage Devices for Texas HHS Confidential Information (as defined in the Texas HHS System Data Use Agreement (DUA))

Cloud Services involve using a network of remote servers hosted on the Internet to store, manage, and process data, rather than a local server or a personal computer.

A Data Center is a centralized repository, either physical or virtual, for the storage, management, and dissemination of data and information organized around a particular body of knowledge or pertaining to a particular business.

Total #
(Sum a-d)

0

a. Devices. Number of personal user computers, devices or drives, including mobile devices and mobile drives.

b. Servers. Number of Servers that are not in a data center or using Cloud Services.

c. Cloud Services. Number of Cloud Services in use.

d. Data Centers. Number of Data Centers in use.

8. Number of unduplicated individuals for whom Applicant/Bidder reasonably expects to handle Texas HHS Confidential Information during one year:

Select Option
(a-d)

a. 499 individuals or less

b. 500 to 999 individuals

c. 1,000 to 99,999 individuals

d. 100,000 individuals or more

- a.
 b.
 c.
 d.

9. HIPAA Business Associate Agreement

a. Will Applicant/Bidder use, disclose, create, receive, transmit or maintain protected health information on behalf of a HIPAA-covered Texas HHS agency for a HIPAA-covered function?

- Yes
 No

b. Does Applicant/Bidder have a Privacy Notice prominently displayed on a Webpage or a Public Office of Applicant/Bidder's business open to or that serves the public? (This is a HIPAA requirement. Answer "N/A" if not applicable, such as for agencies not covered by HIPAA.)

- Yes
 No
 N/A

Action Plan for Compliance with a Timeline:

Compliance Date:

10. Subcontractors. If the Applicant/Bidder responded "0" to Question 4 (indicating no subcontractors), check "N/A" for both 'a.' and 'b.'

a. Does Applicant/Bidder require subcontractors to execute the DUA Attachment 1 Subcontractor Agreement Form?

- Yes
 No
 N/A

Action Plan for Compliance with a Timeline:

Compliance Date:

<p>b. Will Applicant/Bidder agree to require subcontractors who will access Confidential Information to comply with the terms of the DUA, not disclose any Confidential Information to them until they have agreed in writing to the same safeguards and to discontinue their access to the Confidential Information if they fail to comply?</p>	<p> <input type="radio"/> Yes <input type="radio"/> No <input type="radio"/> N/A </p>
<p><u>Action Plan for Compliance with a Timeline:</u></p>	<p><u>Compliance Date:</u></p>
<p>11. Does Applicant/Bidder have any Optional Insurance currently in place?</p> <p>Optional Insurance provides coverage for: (1) Network Security and Privacy; (2) Data Breach; (3) Cyber Liability (lost data, lost use or delay/suspension in business, denial of service with e-business, the Internet, networks and informational assets, such as privacy, intellectual property, virus transmission, extortion, sabotage or web activities); (4) Electronic Media Liability; (5) Crime/Theft; (6) Advertising Injury and Personal Injury Liability; and (7) Crisis Management and Notification Expense Coverage.</p>	<p> <input type="radio"/> Yes <input type="radio"/> No <input type="radio"/> N/A </p>

SECTION B: PRIVACY RISK ANALYSIS AND ASSESSMENT (To be completed by Applicant/Bidder)

For any questions answered "No," an Action Plan for Compliance with a Timeline must be documented in the designated area below the question. The timeline for compliance with HIPAA-related requirements for safeguarding Protected Health Information is 30 calendar days from the date this form is signed. Compliance with requirements related to other types of Confidential Information must be confirmed within 90 calendar days from the date the form is signed.

1. Written Policies & Procedures. Does Applicant/Bidder have current written privacy and security policies and procedures that, at a minimum:	Yes or No
<p>a. Does Applicant/Bidder have current written privacy and security policies and procedures that identify Authorized Users and Authorized Purposes (as defined in the DUA) relating to creation, receipt, maintenance, use, disclosure, access or transmission of Texas HHS Confidential Information?</p>	<input type="radio"/> Yes <input type="radio"/> No
<p><u>Action Plan for Compliance with a Timeline:</u></p>	<p><u>Compliance Date:</u></p>
<p>b. Does Applicant/Bidder have current written privacy and security policies and procedures that require Applicant/Bidder and its Workforce to comply with the applicable provisions of HIPAA and other laws referenced in the DUA, relating to creation, receipt, maintenance, use, disclosure, access or transmission of Texas HHS Confidential Information on behalf of a Texas HHS agency?</p>	<input type="radio"/> Yes <input type="radio"/> No
<p><u>Action Plan for Compliance with a Timeline:</u></p>	<p><u>Compliance Date:</u></p>
<p>c. Does Applicant/Bidder have current written privacy and security policies and procedures that limit use or disclosure of Texas HHS Confidential Information to the minimum that is necessary to fulfill the Authorized Purposes?</p>	<input type="radio"/> Yes <input type="radio"/> No
<p><u>Action Plan for Compliance with a Timeline:</u></p>	<p><u>Compliance Date:</u></p>
<p>d. Does Applicant/Bidder have current written privacy and security policies and procedures that respond to an actual or suspected breach of Texas HHS Confidential Information, to include at a minimum (if any responses are "No" check "No" for all three):</p> <ul style="list-style-type: none"> i. Immediate breach notification to the Texas HHS agency, regulatory authorities, and other required Individuals or Authorities, in accordance with Article 4 of the DUA; ii. Following a documented breach response plan, in accordance with the DUA and applicable law; & iii. Notifying Individuals and Reporting Authorities whose Texas HHS Confidential Information has been breached, as directed by the Texas HHS agency? 	<input type="radio"/> Yes <input type="radio"/> No

<u>Action Plan for Compliance with a Timeline:</u>	<u>Compliance Date:</u>
e. Does Applicant/Bidder have current written privacy and security policies and procedures that conduct annual workforce training and monitoring for and correction of any training delinquencies?	<input type="radio"/> Yes <input type="radio"/> No
<u>Action Plan for Compliance with a Timeline:</u>	<u>Compliance Date:</u>
f. Does Applicant/Bidder have current written privacy and security policies and procedures that permit or deny individual rights of access, and amendment or correction, when appropriate?	<input type="radio"/> Yes <input type="radio"/> No
<u>Action Plan for Compliance with a Timeline:</u>	<u>Compliance Date:</u>
g. Does Applicant/Bidder have current written privacy and security policies and procedures that permit only Authorized Users with up-to-date privacy and security training, and with a reasonable and demonstrable need to use, disclose, create, receive, maintain, access or transmit the Texas HHS Confidential Information, to carry out an obligation under the DUA for an Authorized Purpose, unless otherwise approved in writing by a Texas HHS agency?	<input type="radio"/> Yes <input type="radio"/> No
<u>Action Plan for Compliance with a Timeline:</u>	<u>Compliance Date:</u>
h. Does Applicant/Bidder have current written privacy and security policies and procedures that establish, implement and maintain proof of appropriate sanctions against any Workforce or Subcontractors who fail to comply with an Authorized Purpose or who is not an Authorized User, and used or disclosed Texas HHS Confidential Information in violation of the DUA, the Base Contract or applicable law?	<input type="radio"/> Yes <input type="radio"/> No
<u>Action Plan for Compliance with a Timeline:</u>	<u>Compliance Date:</u>
i. Does Applicant/Bidder have current written privacy and security policies and procedures that require updates to policies, procedures and plans following major changes with use or disclosure of Texas HHS Confidential Information within 60 days of identification of a need for update?	<input type="radio"/> Yes <input type="radio"/> No
<u>Action Plan for Compliance with a Timeline:</u>	<u>Compliance Date:</u>

<p>j. Does Applicant/Bidder have current written privacy and security policies and procedures that restrict permissions or attempts to re-identify or further identify de-identified Texas HHS Confidential Information, or attempt to contact any Individuals whose records are contained in the Texas HHS Confidential Information, except for an Authorized Purpose, without express written authorization from a Texas HHS agency or as expressly permitted by the Base Contract?</p>	<input type="radio"/> Yes <input type="radio"/> No
<p><u>Action Plan for Compliance with a Timeline:</u></p>	<p><u>Compliance Date:</u></p>
<p>k. If Applicant/Bidder intends to use, disclose, create, maintain, store or transmit Texas HHS Confidential Information outside of the United States, will Applicant/Bidder obtain the express prior written permission from the Texas HHS agency and comply with the Texas HHS agency conditions for safeguarding offshore Texas HHS Confidential Information?</p>	<input type="radio"/> Yes <input type="radio"/> No
<p><u>Action Plan for Compliance with a Timeline:</u></p>	<p><u>Compliance Date:</u></p>
<p>l. Does Applicant/Bidder have current written privacy and security policies and procedures that require cooperation with Texas HHS agencies' or federal regulatory inspections, audits or investigations related to compliance with the DUA or applicable law?</p>	<input type="radio"/> Yes <input type="radio"/> No
<p><u>Action Plan for Compliance with a Timeline:</u></p>	<p><u>Compliance Date:</u></p>
<p>m. Does Applicant/Bidder have current written privacy and security policies and procedures that require appropriate standards and methods to destroy or dispose of Texas HHS Confidential Information?</p>	<input type="radio"/> Yes <input type="radio"/> No
<p><u>Action Plan for Compliance with a Timeline:</u></p>	<p><u>Compliance Date:</u></p>
<p>n. Does Applicant/Bidder have current written privacy and security policies and procedures that prohibit disclosure of Applicant/Bidder's work product done on behalf of Texas HHS pursuant to the DUA, or to publish Texas HHS Confidential Information without express prior approval of the Texas HHS agency?</p>	<input type="radio"/> Yes <input type="radio"/> No
<p><u>Action Plan for Compliance with a Timeline:</u></p>	<p><u>Compliance Date:</u></p>
<p>2. Does Applicant/Bidder have a current Workforce training program? Training of Workforce must occur at least once every year, and within 30 days of date of hiring a new Workforce member who will handle Texas HHS Confidential Information. Training must include: (1) privacy and security policies, procedures, plans and applicable requirements for handling Texas HHS Confidential Information, (2) a requirement to complete training before access is given to Texas HHS Confidential Information, and (3) written proof of training and a procedure for monitoring timely completion of training.</p>	<input type="radio"/> Yes <input type="radio"/> No

<u>Action Plan for Compliance with a Timeline:</u>	<u>Compliance Date:</u>
<p>3. Does Applicant/Bidder have Privacy Safeguards to protect Texas HHS Confidential Information in oral, paper and/or electronic form?</p> <p>"Privacy Safeguards" means protection of Texas HHS Confidential Information by establishing, implementing and maintaining required Administrative, Physical and Technical policies, procedures, processes and controls, required by the DUA, HIPAA (45 CFR 164.530), Social Security Administration, Medicaid and laws, rules or regulations, as applicable. Administrative safeguards include administrative protections, policies and procedures for matters such as training, provision of access, termination, and review of safeguards, incident management, disaster recovery plans, and contract provisions. Technical safeguards include technical protections, policies and procedures, such as passwords, logging, emergencies, how paper is faxed or mailed, and electronic protections such as encryption of data. Physical safeguards include physical protections, policies and procedures, such as locks, keys, physical access, physical storage and trash.</p>	<input type="radio"/> Yes <input type="radio"/> No
<u>Action Plan for Compliance with a Timeline:</u>	<u>Compliance Date:</u>
<p>4. Does Applicant/Bidder and all subcontractors (if applicable) maintain a current list of Authorized Users who have access to Texas HHS Confidential Information, whether oral, written or electronic?</p>	<input type="radio"/> Yes <input type="radio"/> No
<u>Action Plan for Compliance with a Timeline:</u>	<u>Compliance Date:</u>
<p>5. Does Applicant/Bidder and all subcontractors (if applicable) monitor for and remove terminated employees or those no longer authorized to handle Texas HHS Confidential Information from the list of Authorized Users?</p>	<input type="radio"/> Yes <input type="radio"/> No
<u>Action Plan for Compliance with a Timeline:</u>	<u>Compliance Date:</u>

SECTION C: SECURITY RISK ANALYSIS AND ASSESSMENT (to be completed by Applicant/Bidder)

<p>This section is about your electronic system. If your business DOES NOT store, access, or transmit Texas HHS Confidential Information in electronic systems (e.g., laptop, personal use computer, mobile device, database, server, etc.) select the box to the right, and "YES" will be entered for all questions in this section.</p>	<p>No Electronic Systems</p> <p><input type="checkbox"/></p>
<p>For any questions answered "No," an Action Plan for Compliance with a Timeline must be documented in the designated area below the question. The timeline for compliance with HIPAA-related items is 30 calendar days, PII-related items is 90 calendar days.</p>	
<p>1. Does the Applicant/Bidder ensure that services which access, create, disclose, receive, transmit, maintain, or store Texas HHS Confidential Information are maintained IN the United States (no offshoring) unless ALL of the following requirements are met?</p> <ul style="list-style-type: none"> a. The data is encrypted with FIPS 140-2 validated encryption b. The offshore provider does not have access to the encryption keys c. The Applicant/Bidder maintains the encryption key within the United States d. The Application/Bidder has obtained the express prior written permission of the Texas HHS agency <p><i>For more information regarding FIPS 140-2 encryption products, please refer to: http://csrc.nist.gov/publications/fips</i></p>	<p><input type="radio"/> Yes</p> <p><input type="radio"/> No</p>
<p><u>Action Plan for Compliance with a Timeline:</u></p>	<p><u>Compliance Date:</u></p>
<p>2. Does Applicant/Bidder utilize an IT security-knowledgeable person or company to maintain or oversee the configurations of Applicant/Bidder's computing systems and devices?</p>	<p><input type="radio"/> Yes</p> <p><input type="radio"/> No</p>
<p><u>Action Plan for Compliance with a Timeline:</u></p>	<p><u>Compliance Date:</u></p>
<p>3. Does Applicant/Bidder monitor and manage access to Texas HHS Confidential Information (e.g., a formal process exists for granting access and validating the need for users to access Texas HHS Confidential Information, and access is limited to Authorized Users)?</p>	<p><input type="radio"/> Yes</p> <p><input type="radio"/> No</p>
<p><u>Action Plan for Compliance with a Timeline:</u></p>	<p><u>Compliance Date:</u></p>
<p>4. Does Applicant/Bidder a) have a system for changing default passwords, b) require user password changes at least every 90 calendar days, and c) prohibit the creation of weak passwords (e.g., require a minimum of 8 characters with a combination of uppercase, lowercase, special characters, and numerals, where possible) for all computer systems that access or store Texas HHS Confidential Information.</p> <p>If yes, upon request must provide evidence such as a screen shot or a system report.</p>	<p><input type="radio"/> Yes</p> <p><input type="radio"/> No</p>
<p><u>Action Plan for Compliance with a Timeline:</u></p>	<p><u>Compliance Date:</u></p>

<p>5. Does each member of Applicant/Bidder's Workforce who will use, disclose, create, receive, transmit or maintain Texas HHS Confidential Information have a unique user name (account) and private password?</p>	<p><input type="radio"/> Yes <input type="radio"/> No</p>
<p><u>Action Plan for Compliance with a Timeline:</u></p>	<p><u>Compliance Date:</u></p>
<p>6. Does Applicant/Bidder lock the password after a certain number of failed attempts and after 15 minutes of user inactivity in all computing devices that access or store Texas HHS Confidential Information?</p>	<p><input type="radio"/> Yes <input type="radio"/> No</p>
<p><u>Action Plan for Compliance with a Timeline:</u></p>	<p><u>Compliance Date:</u></p>
<p>7. Does Applicant/Bidder secure, manage and encrypt remote access (including wireless access) to computer systems containing Texas HHS Confidential Information? (e.g., a formal process exists for granting access and validating the need for users to remotely access Texas HHS Confidential Information, and remote access is limited to Authorized Users).</p> <p><i>Encryption is required for all Texas HHS Confidential Information. Additionally, FIPS 140-2 validated encryption is required for Health Insurance Portability and Accountability Act (HIPAA) data, Criminal Justice Information Services (CJIS) data, Internal Revenue Service Federal Tax Information (IRS FTI) data, and Centers for Medicare & Medicaid Services (CMS) data.</i></p> <p><i>For more information regarding FIPS 140-2 encryption products, please refer to: http://csrc.nist.gov/publications/fips</i></p>	<p><input type="radio"/> Yes <input type="radio"/> No</p>
<p><u>Action Plan for Compliance with a Timeline:</u></p>	<p><u>Compliance Date:</u></p>
<p>8. Does Applicant/Bidder implement computer security configurations or settings for all computers and systems that access or store Texas HHS Confidential Information? (e.g., non-essential features or services have been removed or disabled to reduce the threat of breach and to limit exploitation opportunities for hackers or intruders, etc.)</p>	<p><input type="radio"/> Yes <input type="radio"/> No</p>
<p><u>Action Plan for Compliance with a Timeline:</u></p>	<p><u>Compliance Date:</u></p>
<p>9. Does Applicant/Bidder secure physical access to computer, paper, or other systems containing Texas HHS Confidential Information from unauthorized personnel and theft (e.g., door locks, cable locks, laptops are stored in the trunk of the car instead of the passenger area, etc.)?</p>	<p><input type="radio"/> Yes <input type="radio"/> No</p>
<p><u>Action Plan for Compliance with a Timeline:</u></p>	<p><u>Compliance Date:</u></p>

<p>10. Does Applicant/Bidder use encryption products to protect Texas HHS Confidential Information that is <u>transmitted</u> over a public network (e.g., the Internet, WiFi, etc.)?</p> <p>If yes, upon request must provide evidence such as a screen shot or a system report.</p> <p><i>Encryption is required for all HHS Confidential Information. Additionally, FIPS 140-2 validated encryption is required for Health Insurance Portability and Accountability Act (HIPAA) data, Criminal Justice Information Services (CJIS) data, Internal Revenue Service Federal Tax Information (IRS FTI) data, and Centers for Medicare & Medicaid Services (CMS) data.</i></p> <p><i>For more information regarding FIPS 140-2 encryption products, please refer to: http://csrc.nist.gov/publications/fips</i></p>	<p><input type="radio"/> Yes <input type="radio"/> No</p>
<p><u>Action Plan for Compliance with a Timeline:</u></p>	<p><u>Compliance Date:</u></p>
<p>11. Does Applicant/Bidder use encryption products to protect Texas HHS Confidential Information <u>stored</u> on end user devices (e.g., laptops, USBs, tablets, smartphones, external hard drives, desktops, etc.)?</p> <p>If yes, upon request must provide evidence such as a screen shot or a system report.</p> <p><i>Encryption is required for all Texas HHS Confidential Information. Additionally, FIPS 140-2 validated encryption is required for Health Insurance Portability and Accountability Act (HIPAA) data, Criminal Justice Information Services (CJIS) data, Internal Revenue Service Federal Tax Information (IRS FTI) data, and Centers for Medicare & Medicaid Services (CMS) data.</i></p> <p><i>For more information regarding FIPS 140-2 encryption products, please refer to: http://csrc.nist.gov/publications/fips</i></p>	<p><input type="radio"/> Yes <input type="radio"/> No</p>
<p><u>Action Plan for Compliance with a Timeline:</u></p>	<p><u>Compliance Date:</u></p>
<p>12. Does Applicant/Bidder require Workforce members to formally acknowledge rules outlining their responsibilities for protecting Texas HHS Confidential Information and associated systems containing HHS Confidential Information before their access is provided?</p>	<p><input type="radio"/> Yes <input type="radio"/> No</p>
<p><u>Action Plan for Compliance with a Timeline:</u></p>	<p><u>Compliance Date:</u></p>
<p>13. Is Applicant/Bidder willing to perform or submit to a criminal background check on Authorized Users?</p>	<p><input type="radio"/> Yes <input type="radio"/> No</p>
<p><u>Action Plan for Compliance with a Timeline:</u></p>	<p><u>Compliance Date:</u></p>
<p>14. Does Applicant/Bidder prohibit the access, creation, disclosure, reception, transmission, maintenance, and storage of Texas HHS Confidential Information with a subcontractor (e.g., cloud services, social media, etc.) unless Texas HHS has approved the subcontractor agreement which must include compliance and liability clauses with the same requirements as the Applicant/Bidder?</p>	<p><input type="radio"/> Yes <input type="radio"/> No</p>
<p><u>Action Plan for Compliance with a Timeline:</u></p>	<p><u>Compliance Date:</u></p>

15. Does Applicant/Bidder keep current on security updates/patches (including firmware, software and applications) for computing systems that use, disclose, access, create, transmit, maintain or store Texas HHS Confidential Information?	<input type="radio"/> Yes <input type="radio"/> No
<u>Action Plan for Compliance with a Timeline:</u>	<u>Compliance Date:</u>
16. Do Applicant/Bidder's computing systems that use, disclose, access, create, transmit, maintain or store Texas HHS Confidential Information contain up-to-date anti-malware and antivirus protection?	<input type="radio"/> Yes <input type="radio"/> No
<u>Action Plan for Compliance with a Timeline:</u>	<u>Compliance Date:</u>
17. Does the Applicant/Bidder review system security logs on computing systems that access or store Texas HHS Confidential Information for abnormal activity or security concerns on a regular basis?	<input type="radio"/> Yes <input type="radio"/> No
<u>Action Plan for Compliance with a Timeline:</u>	<u>Compliance Date:</u>
18. Notwithstanding records retention requirements, does Applicant/Bidder's disposal processes for Texas HHS Confidential Information ensure that Texas HHS Confidential Information is destroyed so that it is unreadable or undecipherable?	<input type="radio"/> Yes <input type="radio"/> No
<u>Action Plan for Compliance with a Timeline:</u>	<u>Compliance Date:</u>
19. Does the Applicant/Bidder ensure that all public facing websites and mobile applications containing Texas HHS Confidential Information meet security testing standards set forth within the Texas Government Code (TGC), Section 2054.516; including requirements for implementing vulnerability and penetration testing and addressing identified vulnerabilities? <i>For more information regarding TGC, Section 2054.516 DATA SECURITY PLAN FOR ONLINE AND MOBILE APPLICATIONS, please refer to: https://legiscan.com/TX/text/HB8/2017</i>	<input type="radio"/> Yes <input type="radio"/> No
<u>Action Plan for Compliance with a Timeline:</u>	<u>Compliance Date:</u>

SECTION D: SIGNATURE AND SUBMISSION (to be completed by Applicant/Bidder)

Please sign the form digitally, if possible. If you can't, provide a handwritten signature.

1. I certify that all of the information provided in this form is truthful and correct to the best of my knowledge. If I learn that any such information was not correct, I agree to notify Texas HHS of this immediately.

2. Signature	3. Title	4. Date:
---------------------	-----------------	-----------------

To **submit** the completed, signed form:

- Email the form as an attachment to the appropriate Texas HHS Contract Manager(s).

Section E: To Be Completed by Texas HHS Agency Staff:

Agency(s): HHSC: <input type="checkbox"/> DFPS: <input type="checkbox"/> DSHS: <input type="checkbox"/>	Requesting Department(s): 								
Legal Entity Tax Identification Number (TIN) (Last four Only): <table style="width:100%; border-collapse: collapse;"> <tr> <td style="width:25%; background-color: #cccccc;"> </td> <td style="width:25%; background-color: #cccccc;"> </td> <td style="width:25%; background-color: #cccccc;"> </td> <td style="width:25%; background-color: #cccccc;"> </td> <td style="width:25%; border: 1px solid black;"> </td> <td style="width:25%; border: 1px solid black;"> </td> <td style="width:25%; border: 1px solid black;"> </td> <td style="width:25%; border: 1px solid black;"> </td> </tr> </table>									PO/Contract(s) #:

Contract Manager:	Contract Manager Email Address:	Contract Manager Telephone #:
Contract Manager:	Contract Manager Email Address:	Contract Manager Telephone #:
Contract Manager:	Contract Manager Email Address:	Contract Manager Telephone #:
Contract Manager:	Contract Manager Email Address:	Contract Manager Telephone #:
Contract Manager:	Contract Manager Email Address:	Contract Manager Telephone #:
Contract Manager:	Contract Manager Email Address:	Contract Manager Telephone #:
Contract Manager:	Contract Manager Email Address:	Contract Manager Telephone #:
Contract Manager:	Contract Manager Email Address:	Contract Manager Telephone #:

INSTRUCTIONS FOR COMPLETING THE SECURITY AND PRIVACY INQUIRY (SPI)

Below are instructions for Applicants, Bidders and Contractors for Texas Health and Human Services requiring the Attachment 2, Security and Privacy Inquiry (SPI) to the Data Use Agreement (DUA). Instruction item numbers below correspond to sections on the SPI form.

If you are a bidder for a new procurement/contract, in order to participate in the bidding process, you must have corrected any "No" responses (except A9a) prior to the contract award date. If you are an applicant for an open enrollment, you must have corrected any "No" answers (except A9a and A11) prior to performing any work on behalf of any Texas HHS agency.

For any questions answered "No" (except A9a and A11), an *Action Plan for Compliance with a Timeline* must be documented in the designated area below the question. The timeline for compliance with HIPAA-related requirements for safeguarding Protected Health Information is 30 calendar days from the date this form is signed. Compliance with requirements related to other types of Confidential Information must be confirmed within 90 calendar days from the date the form is signed.

SECTION A. APPLICANT /BIDDER INFORMATION

Item #1. *Only contractors that access, transmit, store, and/or maintain Texas HHS Confidential Information will complete and email this form as an attachment to the appropriate Texas HHS Contract Manager.*

Item #2. Entity or Applicant/Bidder Legal Name. *Provide the legal name of the business (the name used for legal purposes, like filing a federal or state tax form on behalf of the business, and is not a trade or assumed named "dba"), the legal tax identification number (last four numbers only) of the entity or applicant/bidder, the address of the corporate or main branch of the business, the telephone number where the business can be contacted regarding questions related to the information on this form and the website of the business, if a website exists.*

Item #3. Number of Employees, at all locations, in Applicant/Bidder's workforce. *Provide the total number of individuals, including volunteers, subcontractors, trainees, and other persons who work for the business. If you are the only employee, please answer "1."*

Item #4. Number of Subcontractors. *Provide the total number of subcontractors working for the business. If you have none, please answer "0" zero.*

Item #5. Number of unduplicated individuals for whom Applicant/Bidder reasonably expects to handle HHS Confidential Information during one year. *Select the radio button that corresponds with the number of clients/consumers for whom you expect to handle Texas HHS Confidential Information during a year. Only count clients/consumers once, no matter how many direct services the client receives during a year.*

Item #5. Name of Information Technology Security Official and Name of Privacy Official for Applicant/Bidder. *As with all other fields on the SPI, this is a required field. This may be the same person and the owner of the business if such person has the security and privacy knowledge that is required to implement the requirements of the DUA and respond to questions related to the SPI. In 4.A. provide the name, address, telephone number, and email address of the person whom you have designated to answer any security questions found in Section C and in 4.B. provide this information for the person whom you have designated as the person to answer any privacy questions found in Section B. The business may contract out for this expertise; however, designated individual(s) must have knowledge of the business's devices, systems and methods for use, disclosure, creation, receipt, transmission and maintenance of Texas HHS Confidential Information and be willing to be the point of contact for privacy and security questions.*

Item #6. Type(s) of HHS Confidential Information the Entity or Applicant/Bidder Will Create, Receive, Maintain, Use, Disclose or Have Access to: *Provide a complete listing of all Texas HHS Confidential Information that the Contractor will create, receive, maintain, use, disclose or have access to. The DUA section Article 2, Definitions, defines Texas HHS Confidential Information as:*

"Confidential Information" means any communication or record (whether oral, written, electronically stored or transmitted, or in any other form) provided to or made available to CONTRACTOR or that CONTRACTOR may create, receive, maintain, use, disclose or have access to on behalf of Texas HHS that consists of or includes any or all of the following:

- (1) Client Information;*
- (2) Protected Health Information in any form including without limitation, Electronic Protected Health Information or Unsecured Protected Health Information;*
- (3) Sensitive Personal Information defined by Texas Business and Commerce Code Ch. 521;*

(4) Federal Tax Information;

(5) Personally Identifiable Information;

(6) Social Security Administration Data, including, without limitation, Medicaid information;

(7) All privileged work product;

(8) All information designated as confidential under the constitution and laws of the State of Texas and of the United States, including the Texas Health & Safety Code and the Texas Public Information Act, Texas Government Code, Chapter 552.

Definitions for the following types of confidential information can be found the following sites:

- Health Insurance Portability and Accountability Act (HIPAA) - <http://www.hhs.gov/hipaa/index.html>
- Criminal Justice Information Services (CJIS) - <https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center>
- Internal Revenue Service Federal Tax Information (IRS FTI) - <https://www.irs.gov/pub/irs-pdf/p1075.pdf>
- Centers for Medicare & Medicaid Services (CMS) - <https://www.cms.gov/Regulations-and-Guidance/Regulations-and-Guidance.html>
- Social Security Administration (SSA) - <https://www.ssa.gov/regulations/>
- Personally Identifiable Information (PII) - <http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf>

Item #7. Number of Storage devices for Texas HHS Confidential Information. The total number of devices is automatically calculated by exiting the fields in lines a - d. Use the <Tab> key when exiting the field to prompt calculation, if it doesn't otherwise sum correctly.

- **Item 7a. Devices.** Provide the number of personal user computers, devices, and drives (including mobile devices, laptops, USB drives, and external drives) on which your business stores or will store Texas HHS Confidential Information.
- **Item 7b. Servers.** Provide the number of servers not housed in a data center or "in the cloud," on which Texas HHS Confidential Information is stored or will be stored. A server is a dedicated computer that provides data or services to other computers. It may provide services or data to systems on a local area network (LAN) or a wide area network (WAN) over the Internet. If none, answer "0" (zero).
- **Item 7c. Cloud Services.** Provide the number of cloud services to which Texas HHS Confidential Information is stored. Cloud Services involve using a network of remote servers hosted on the Internet to store, manage, and process data, rather than on a local server or a personal computer. If none, answer "0" (zero.)
- **Item 7d. Data Centers.** Provide the number of data centers in which you store Texas HHS Confidential Information. A Data Center is a centralized repository, either physical or virtual, for the storage, management, and dissemination of data and information organized around a particular body of knowledge or pertaining to a particular business. If none, answer "0" (zero).

Item #8. Number of unduplicated individuals for whom the Applicant/Bidder reasonably expects to handle Texas HHS Confidential Information during one year. Select the radio button that corresponds with the number of clients/consumers for whom you expect to handle Confidential Information during a year. Only count clients/consumers once, no matter how many direct services the client receives during a year.

Item #9. HIPAA Business Associate Agreement.

- **Item #9a.** Answer "Yes" if your business will use, disclose, create, receive, transmit, or store information relating to a client/consumer's healthcare on behalf of the Department of State Health Services, the Department of Disability and Aging Services, or the Health and Human Services Commission for treatment, payment, or operation of Medicaid or Medicaid clients. If your contract does not include HIPAA covered information, respond "no." If "no," a compliance plan is not required.
- **Item #9b.** Answer "Yes" if your business has a notice of privacy practices (a document that explains how you protect and use a client/consumer's healthcare information) displayed either on a website (if one exists for your business) or in your place of business (if that location is open to clients/consumers or the public). If your contract does not include HIPAA covered information, respond "N/A."

Item #10. Subcontractors. If your business responded "0" to question 4 (number of subcontractors), Answer "N/A" to Items 10a and 10b to indicate not applicable.

- **Item #10a.** Answer "Yes" if your business requires that all subcontractors sign Attachment 1 of the DUA.
- **Item #10b.** Answer "Yes" if your business obtains Texas HHS approval before permitting subcontractors to handle Texas HHS Confidential Information on your business's behalf.

Item #11. Optional Insurance. Answer "yes" if applicant has optional insurance in place to provide coverage for a Breach or any

SECTION B. PRIVACY RISK ANALYSIS AND ASSESSMENT

Reasonable and appropriate written Privacy and Security policies and procedures are required, even for sole proprietors who are the only employee, to demonstrate how your business will safeguard Texas HHS Confidential Information and respond in the event of a Breach of Texas HHS Confidential Information. To ensure that your business is prepared, all of the items below must be addressed in your written Privacy and Security policies and procedures.

Item #1. Answer "Yes" if you have written policies in place for each of the areas (a-o).

- **Item #1a.** Answer "yes" if your business has written policies and procedures that identify everyone, including subcontractors, who are authorized to use Texas HHS Confidential Information. The policies and procedures should also identify the reason why these Authorized Users need to access the Texas HHS Confidential Information and this reason must align with the Authorized Purpose described in the Scope of Work or description of services in the Base Contract with the Texas HHS agency.
- **Item #1b.** Answer "Yes" if your business has written policies and procedures that require your employees (including yourself), your volunteers, your trainees, and any other persons whose work you direct, to comply with the requirements of HIPAA, if applicable, and other confidentiality laws as they relate to your handling of Texas HHS Confidential Information. Refer to the laws and rules that apply, including those referenced in the DUA and Scope of Work or description of services in the Base Contract.
- **Item #1c.** Answer "Yes" if your business has written policies and procedures that limit the Texas HHS Confidential Information you disclose to the minimum necessary for your workforce and subcontractors (if applicable) to perform the obligations described in the Scope of Work or service description in the Base Contract. (e.g., if a client/consumer's Social Security Number is not required for a workforce member to perform the obligations described in the Scope of Work or service description in the Base Contract, then the Social Security Number will not be given to them.) If you are the only employee for your business, policies and procedures must not include a request for, or use of, Texas HHS Confidential Information that is not required for performance of the services.
- **Item #1d.** Answer "Yes" if your business has written policies and procedures that explain how your business would respond to an actual or suspected breach of Texas HHS Confidential Information. The written policies and procedures, at a minimum, must include the three items below. If any response to the three items below are no, answer "no."
 - **Item #1di.** Answer "Yes" if your business has written policies and procedures that require your business to immediately notify Texas HHS, the Texas HHS Agency, regulatory authorities, or other required Individuals or Authorities of a Breach as described in Article 4, Section 4 of the DUA.
Refer to Article 4, Section 4.01:
Initial Notice of Breach must be provided in accordance with Texas HHS and DUA requirements with as much information as possible about the Event/Breach and a name and contact who will serve as the single point of contact with HHS both on and off business hours. Time frames related to Initial Notice include:
 - *within one hour of Discovery of an Event or Breach of Federal Tax Information, Social Security Administration Data, or Medicaid Client Information*
 - *within 24 hours of all other types of Texas HHS Confidential Information **48-hour Formal Notice** must be provided no later than 48 hours after Discovery for protected health information, sensitive personal information or other non-public information and must include applicable information as referenced in Section 4.01 (C) 2. of the DUA.*
 - **Item #1dii.** Answer "Yes" if your business has written policies and procedures require you to have and follow a written breach response plan as described in Article 4 Section 4.02 of the DUA.
 - **Item #1diii.** Answer "Yes" if your business has written policies and procedures require you to notify Reporting Authorities and Individuals whose Texas HHS Confidential Information has been breached as described in Article 4 Section 4.03 of the DUA.
- **Item #1e.** Answer "Yes" if your business has written policies and procedures requiring annual training of your entire workforce on matters related to confidentiality, privacy, and security, stressing the importance of promptly reporting any Event or Breach, outlines the process that you will use to require attendance and track completion for employees who failed to complete annual training.

- **Item #1f.** Answer "Yes" if your business has written policies and procedures requiring you to allow individuals (clients/consumers) to access their individual record of Texas HHS Confidential Information, and allow them to amend or correct that information, if applicable.
- **Item #1g.** Answer "Yes" if your business has written policies and procedures restricting access to Texas HHS Confidential Information to only persons who have been authorized and trained on how to handle Texas HHS Confidential Information
- **Item #1h.** Answer "Yes" if your business has written policies and procedures requiring sanctioning of any subcontractor, employee, trainee, volunteer, or anyone whose work you direct when they have accessed Texas HHS Confidential Information but are not authorized to do so, and that you have a method of proving that you have sanctioned such an individuals. If you are the only employee, you must demonstrate how you will document the noncompliance, update policies and procedures if needed, and seek additional training or education to prevent future occurrences.
- **Item #1i.** Answer "Yes" if your business has written policies and procedures requiring you to update your policies within 60 days after you have made changes to how you use or disclose Texas HHS Confidential Information.
- **Item #1j.** Answer "Yes" if your business has written policies and procedures requiring you to restrict attempts to take de-identified data and re-identify it or restrict any subcontractor, employee, trainee, volunteer, or anyone whose work you direct, from contacting any individuals for whom you have Texas HHS Confidential Information except to perform obligations under the contract, or with written permission from Texas HHS.
- **Item #1k.** Answer "Yes" if your business has written policies and procedures prohibiting you from using, disclosing, creating, maintaining, storing or transmitting Texas HHS Confidential Information outside of the United States.
- **Item #1l.** Answer "Yes" if your business has written policies and procedures requiring your business to cooperate with HHS agencies or federal regulatory entities for inspections, audits, or investigations related to compliance with the DUA or applicable law.
- **Item #1m.** Answer "Yes" if your business has written policies and procedures requiring your business to use appropriate standards and methods to destroy or dispose of Texas HHS Confidential Information. Policies and procedures should comply with Texas HHS requirements for retention of records and methods of disposal.
- **Item #1n.** Answer "Yes" if your business has written policies and procedures prohibiting the publication of the work you created or performed on behalf of Texas HHS pursuant to the DUA, or other Texas HHS Confidential Information, without express prior written approval of the HHS agency.

Item #2. Answer "Yes" if your business has a current training program that meets the requirements specified in the SPI for you, your employees, your subcontractors, your volunteers, your trainees, and any other persons under you direct supervision.

Item #3. Answer "Yes" if your business has privacy safeguards to protect Texas HHS Confidential Information as described in the SPI.

Item #4. Answer "Yes" if your business maintains current lists of persons in your workforce, including subcontractors (if applicable), who are authorized to access Texas HHS Confidential Information. If you are the only person with access to Texas HHS Confidential Information, please answer "yes."

Item #5. Answer "Yes" if your business and subcontractors (if applicable) monitor for and remove from the list of Authorized Users, members of the workforce who are terminated or are no longer authorized to handle Texas HHS Confidential Information. If you are the only one with access to Texas HHS Confidential Information, please answer "Yes."

SECTION C. SECURITY RISK ANALYSIS AND ASSESSMENT

This section is about your electronic systems. If you DO NOT store Texas HHS Confidential Information in electronic systems (e.g., laptop, personal computer, mobile device, database, server, etc.), select the "No Electronic Systems" box and respond "Yes" for all questions in this section.

Item #1. Answer "Yes" if your business does not "offshore" or use, disclose, create, receive, transmit or maintain Texas HHS Confidential Information outside of the United States. If you are not certain, contact your provider of technology services (application, cloud, data center, network, etc.) and request confirmation that they do not offshore their data.

Item #2. Answer "Yes" if your business uses a person or company who is knowledgeable in IT security to maintain or oversee the configurations of your business's computing systems and devices. You may be that person, or you may hire someone who can provide that service for you.

Item #3. Answer "Yes" if your business monitors and manages access to Texas HHS Confidential Information (i.e., reviews systems to ensure that access is limited to Authorized Users; has formal processes for granting, validating, and reviews the need for remote access to Authorized Users to Texas HHS Confidential Information, etc.). If you are the only employee, answer "Yes" if you have implemented a process to periodically evaluate the need for accessing Texas HHS Confidential Information to fulfill your Authorized Purposes.

Item #4. Answer "Yes" if your business has implemented a system for changing the password a system initially assigns to the user (also known as the default password), and requires users to change their passwords at least every 90 days, and prohibits the creation of weak passwords for all computer systems that access or store Texas HHS Confidential Information (e.g., a strong password has a minimum of 8 characters with a combination of uppercase, lowercase, special characters, and numbers, where possible). If your business uses a Microsoft Windows system, refer to the Microsoft website on how to do this, see example: <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/password-policy>

Item #5. Answer "Yes" if your business assigns a unique user name and private password to each of your employees, your subcontractors, your volunteers, your trainees and any other persons under your direct control who will use, disclose, create, receive, transmit or maintain Texas HHS Confidential Information.

Item #6. Answer "Yes" if your business locks the access after a certain number of failed attempts to login and after 15 minutes of user inactivity on all computing devices that access or store Texas HHS Confidential Information. If your business uses a Microsoft Windows system, refer to the Microsoft website on how to do this, see example: <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/account-lockout-policy>

Item #7. Answer "Yes" if your business secures, manages, and encrypts remote access, such as: using Virtual Private Network (VPN) software on your home computer to access Texas HHS Confidential Information that resides on a computer system at a business location or, if you use wireless, ensuring that the wireless is secured using a password code. If you do not access systems remotely or over wireless, answer "Yes."

Item #8. Answer "Yes" if your business updates the computer security settings for all your computers and electronic systems that access or store Texas HHS Confidential Information to prevent hacking or breaches (e.g., non-essential features or services have been removed or disabled to reduce the threat of breach and to limit opportunities for hackers or intruders to access your system). For example, Microsoft's Windows security checklist: <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/how-to-configure-security-policy-settings>

Item #9. Answer "Yes" if your business secures physical access to computer, paper, or other systems containing Texas HHS Confidential Information from unauthorized personnel and theft (e.g., door locks, cable locks, laptops are stored in the trunk of the car instead of the passenger area, etc.). If you are the only employee and use these practices for your business, answer "Yes."

Item #10. Answer "Yes" if your business uses encryption products to protect Texas HHS Confidential Information that is transmitted over a public network (e.g., the Internet, WIFI, etc.) or that is stored on a computer system that is physically or electronically accessible to the public (FIPS 140-2 validated encryption is required for Health Insurance Portability and Accountability Act (HIPAA) data, Criminal Justice Information Services (CJIS) data, Internal Revenue Service Federal Tax Information (IRS FTI) data, and Centers for Medicare & Medicaid Services (CMS) data.) For more information regarding FIPS 140-2 encryption products, please refer to: <http://csrc.nist.gov/publications/fips>).

Item #11. Answer "Yes" if your business stores Texas HHS Confidential Information on encrypted end-user electronic devices (e.g., laptops, USBs, tablets, smartphones, external hard drives, desktops, etc.) and can produce evidence of the encryption, such as, a screen shot or a system report (FIPS 140-2 encryption is required for Health Insurance Portability and Accountability Act (HIPAA) data, Criminal Justice Information Services (CJIS) data, Internal Revenue Service Federal Tax Information (IRS FTI) data, and Centers for Medicare & Medicaid Services (CMS) data). For more information regarding FIPS 140-2 validated encryption products, please refer to: <http://csrc.nist.gov/publications/fips>). If you do not utilize end-user electronic devices for storing Texas HHS Confidential Information, answer "Yes."

Item #12. Answer "Yes" if your business requires employees, volunteers, trainees and other workforce members to sign a document that clearly outlines their responsibilities for protecting Texas HHS Confidential Information and associated systems containing Texas HHS Confidential Information before they can obtain access. If you are the only employee answer "Yes" if you have signed or are willing to sign the DUA, acknowledging your adherence to requirements and responsibilities.

Item #13. Answer "Yes" if your business is willing to perform a criminal background check on employees, subcontractors, volunteers, or trainees who access Texas HHS Confidential Information. If you are the only employee, answer "Yes" if you are willing to submit to a background check.

Item #14. Answer "Yes" if your business prohibits the access, creation, disclosure, reception, transmission, maintenance, and storage of Texas HHS Confidential Information on Cloud Services or social media sites if you use such services or sites, and there is a Texas HHS approved subcontractor agreement that includes compliance and liability clauses with the same requirements as the Applicant/Bidder. If you do not utilize Cloud Services or media sites for storing Texas HHS Confidential Information, answer "Yes."

Item #15. Answer "Yes" if your business keeps current on security updates/patches (including firmware, software and applications) for computing systems that use, disclose, access, create, transmit, maintain or store Texas HHS Confidential Information. If you use a Microsoft Windows system, refer to the Microsoft website on how to ensure your system is automatically updating, see example:

<https://portal.msrc.microsoft.com/en-us/>

Item #16. Answer "Yes" if your business's computing systems that use, disclose, access, create, transmit, maintain or store Texas HHS Confidential Information contain up-to-date anti-malware and antivirus protection. If you use a Microsoft Windows system, refer to the Microsoft website on how to ensure your system is automatically updating, see example:

<https://docs.microsoft.com/en-us/windows/security/threat-protection/>

Item #17. Answer "Yes" if your business reviews system security logs on computing systems that access or store Texas HHS Confidential Information for abnormal activity or security concerns on a regular basis. If you use a Microsoft Windows system, refer to the Microsoft website for ensuring your system is logging security events, see example:

<https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/basic-security-audit-policies>

Item #18. Answer "Yes" if your business disposal processes for Texas HHS Confidential Information ensures that Texas HHS Confidential Information is destroyed so that it is unreadable or undecipherable. Simply deleting data or formatting the hard drive is not enough; ensure you use products that perform a secure disk wipe. Please see NIST SP 800-88 R1, *Guidelines for Media Sanitization* and the applicable laws and regulations for the information type for further guidance.

Item #19. Answer "Yes" if your business ensures that all public facing websites and mobile applications containing HHS Confidential Information meet security testing standards set forth within the Texas Government Code (TGC), Section 2054.516

SECTION D. SIGNATURE AND SUBMISSION

Click on the signature area to digitally sign the document. Email the form as an attachment to the appropriate Texas HHS Contract Manager.

Certificate Of Completion

Envelope Id: 043ABD073CC6498EA38262FA19F37A62	Status: Completed
Subject: HHS000812700042, Corpus Christi-Nueces County Public Health District (City), IDCU/COVID Contract	
Source Envelope:	
Document Pages: 92	Signatures: 6
Certificate Pages: 6	Initials: 0
AutoNav: Enabled	Envelope Originator:
Envelopeld Stamping: Enabled	CMS Internal Routing Mailbox
Time Zone: (UTC-06:00) Central Time (US & Canada)	11493 Sunset Hills Road
	#100
	Reston, VA 20190
	CMS.InternalRouting@dshs.texas.gov
	IP Address: 160.42.85.9

Record Tracking

Status: Original	Holder: CMS Internal Routing Mailbox	Location: DocuSign
5/3/2022 3:58:03 PM	CMS.InternalRouting@dshs.texas.gov	

Signer Events

Steven Viera
 stevev@cctexas.com
 Interim Director of Health
 Corpus Christi - Nueces County Public Health
 Security Level: Email, Account Authentication (None)

Signature

DocuSigned by:

 7A188293F923439...
 Signature Adoption: Pre-selected Style
 Signed by link sent to stevev@cctexas.com
 Using IP Address: 155.190.8.4

Timestamp

Sent: 5/3/2022 4:02:37 PM
 Viewed: 5/3/2022 4:19:04 PM
 Signed: 5/16/2022 1:58:40 PM

Electronic Record and Signature Disclosure:

Accepted: 3/1/2022 5:00:47 PM
 ID: 4f8f2f59-1a8a-43c3-a675-dd40eae6c04f

Susana Garcia
 Susana.Garcia@dshs.texas.gov
 CTCM, Unit Director
 DSHS
 Security Level: Email, Account Authentication (None)

Completed

Signed by link sent to
 Susana.Garcia@dshs.texas.gov
 Using IP Address: 167.137.1.12

Sent: 5/16/2022 1:58:43 PM
 Resent: 5/27/2022 12:43:55 PM
 Viewed: 6/7/2022 9:58:06 AM
 Signed: 6/13/2022 10:09:38 AM

Electronic Record and Signature Disclosure:

Accepted: 6/13/2022 10:08:31 AM
 ID: aeab3013-6734-42aa-a5e4-afcc8dcf0c0e

PATTY MELCHIOR
 Patty.Melchior@dshs.texas.gov
 Director, DSHS CMS
 Security Level: Email, Account Authentication (None)


Completed

Signed by link sent to
 Patty.Melchior@dshs.texas.gov
 Using IP Address: 167.137.1.17

Sent: 6/13/2022 10:09:41 AM
 Resent: 6/13/2022 10:10:17 AM
 Viewed: 6/13/2022 10:30:12 AM
 Signed: 6/13/2022 10:31:40 AM

Electronic Record and Signature Disclosure:

Accepted: 5/5/2022 12:43:08 PM
 ID: f01589da-43a7-481e-996a-7c50409e5d48

Signer Events	Signature	Timestamp
<p>Imelda Garcia ImeldaM.Garcia@dshs.texas.gov Associate Commissioner Texas Health and Human Services Commission Security Level: Email, Account Authentication (None)</p> <p>Electronic Record and Signature Disclosure: Accepted: 7/6/2021 8:08:45 AM ID: 1a6909aa-b026-45a9-be9f-4240c2e32ff9</p>	<p>DocuSigned by:  87AFD32AD9D24A9...</p> <p>Signature Adoption: Pre-selected Style Signed by link sent to ImeldaM.Garcia@dshs.texas.gov Using IP Address: 160.42.85.12 Signed using mobile</p>	<p>Sent: 6/13/2022 10:31:43 AM Viewed: 6/13/2022 10:42:26 AM Signed: 6/13/2022 10:42:38 AM</p>

In Person Signer Events	Signature	Timestamp
-------------------------	-----------	-----------

Editor Delivery Events	Status	Timestamp
------------------------	--------	-----------

Agent Delivery Events	Status	Timestamp
-----------------------	--------	-----------

Intermediary Delivery Events	Status	Timestamp
------------------------------	--------	-----------

Certified Delivery Events	Status	Timestamp
---------------------------	--------	-----------

Carbon Copy Events	Status	Timestamp
--------------------	--------	-----------

<p>Moriam Ojelade moriamO@cctexas.com Security Level: Email, Account Authentication (None)</p> <p>Electronic Record and Signature Disclosure: Not Offered via DocuSign</p>	<div style="border: 2px solid blue; padding: 5px; font-weight: bold; color: blue; font-size: 1.2em;">COPIED</div>	<p>Sent: 5/3/2022 4:02:36 PM</p>
--	---	----------------------------------

<p>Raymond Maylone RaymondM2@cctexas.com Security Level: Email, Account Authentication (None)</p> <p>Electronic Record and Signature Disclosure: Not Offered via DocuSign</p>	<div style="border: 2px solid blue; padding: 5px; font-weight: bold; color: blue; font-size: 1.2em;">COPIED</div>	<p>Sent: 5/3/2022 4:02:36 PM Viewed: 5/3/2022 4:07:35 PM</p>
---	---	---

<p>Caeli Paradise caeli.paradise@dshs.texas.gov Contract Manager Security Level: Email, Account Authentication (None)</p> <p>Electronic Record and Signature Disclosure: Accepted: 12/21/2021 2:35:07 PM ID: c6dab47b-ff17-4990-be85-4057f6a41671</p>	<div style="border: 2px solid blue; padding: 5px; font-weight: bold; color: blue; font-size: 1.2em;">COPIED</div>	<p>Sent: 5/3/2022 4:02:36 PM Viewed: 6/13/2022 11:03:00 AM</p>
---	---	---

<p>Denzel Otokunrin denzelo@cctexas.com Security Level: Email, Account Authentication (None)</p> <p>Electronic Record and Signature Disclosure: Not Offered via DocuSign</p>	<div style="border: 2px solid blue; padding: 5px; font-weight: bold; color: blue; font-size: 1.2em;">COPIED</div>	<p>Sent: 5/3/2022 4:02:35 PM</p>
--	---	----------------------------------

<p>CMS Internal Routing Mailbox CMS.InternalRouting@dshs.texas.gov DSHS Contract Management Section Security Level: Email, Account Authentication (None)</p> <p>Electronic Record and Signature Disclosure: Not Offered via DocuSign</p>	<div style="border: 2px solid blue; padding: 5px; font-weight: bold; color: blue; font-size: 1.2em;">COPIED</div>	<p>Sent: 6/13/2022 10:42:42 AM Resent: 6/13/2022 10:42:45 AM</p>
---	---	---

Witness Events	Signature	Timestamp
-----------------------	------------------	------------------

Notary Events	Signature	Timestamp
----------------------	------------------	------------------

Envelope Summary Events	Status	Timestamps
--------------------------------	---------------	-------------------

Envelope Sent	Hashed/Encrypted	5/3/2022 4:02:36 PM
Certified Delivered	Security Checked	6/13/2022 10:42:26 AM
Signing Complete	Security Checked	6/13/2022 10:42:38 AM
Completed	Security Checked	6/13/2022 10:42:42 AM

Payment Events	Status	Timestamps
-----------------------	---------------	-------------------

Electronic Record and Signature Disclosure

ELECTRONIC RECORD AND SIGNATURE DISCLOSURE

From time to time, DSHS Contract Management Section (we, us or Company) may be required by law to provide to you certain written notices or disclosures. Described below are the terms and conditions for providing to you such notices and disclosures electronically through the DocuSign system. Please read the information below carefully and thoroughly, and if you can access this information electronically to your satisfaction and agree to this Electronic Record and Signature Disclosure (ERSD), please confirm your agreement by selecting the check-box next to 'I agree to use electronic records and signatures' before clicking 'CONTINUE' within the DocuSign system.

Getting paper copies

At any time, you may request from us a paper copy of any record provided or made available electronically to you by us. You will have the ability to download and print documents we send to you through the DocuSign system during and immediately after the signing session and, if you elect to create a DocuSign account, you may access the documents for a limited period of time (usually 30 days) after such documents are first sent to you. After such time, if you wish for us to send you paper copies of any such documents from our office to you, you will be charged a \$0.00 per-page fee. You may request delivery of such paper copies from us by following the procedure described below.

Withdrawing your consent

If you decide to receive notices and disclosures from us electronically, you may at any time change your mind and tell us that thereafter you want to receive required notices and disclosures only in paper format. How you must inform us of your decision to receive future notices and disclosure in paper format and withdraw your consent to receive notices and disclosures electronically is described below.

Consequences of changing your mind

If you elect to receive required notices and disclosures only in paper format, it will slow the speed at which we can complete certain steps in transactions with you and delivering services to you because we will need first to send the required notices or disclosures to you in paper format, and then wait until we receive back from you your acknowledgment of your receipt of such paper notices or disclosures. Further, you will no longer be able to use the DocuSign system to receive required notices and consents electronically from us or to sign electronically documents from us.

All notices and disclosures will be sent to you electronically

Unless you tell us otherwise in accordance with the procedures described herein, we will provide electronically to you through the DocuSign system all required notices, disclosures, authorizations, acknowledgements, and other documents that are required to be provided or made available to you during the course of our relationship with you. To reduce the chance of you inadvertently not receiving any notice or disclosure, we prefer to provide all of the required notices and disclosures to you by the same method and to the same address that you have given us. Thus, you can receive all the disclosures and notices electronically or in paper format through the paper mail delivery system. If you do not agree with this process, please let us know as described below. Please also see the paragraph immediately above that describes the consequences of your electing not to receive delivery of the notices and disclosures electronically from us.

How to contact DSHS Contract Management Section:

You may contact us to let us know of your changes as to how we may contact you electronically, to request paper copies of certain information from us, and to withdraw your prior consent to receive notices and disclosures electronically as follows:

To contact us by email send messages to: alison.joffrion@hhsc.state.tx.us

To advise DSHS Contract Management Section of your new email address

To let us know of a change in your email address where we should send notices and disclosures electronically to you, you must send an email message to us at alison.joffrion@hhsc.state.tx.us and in the body of such request you must state: your previous email address, your new email address. We do not require any other information from you to change your email address.

If you created a DocuSign account, you may update it with your new email address through your account preferences.

To request paper copies from DSHS Contract Management Section

To request delivery from us of paper copies of the notices and disclosures previously provided by us to you electronically, you must send us an email to alison.joffrion@hhsc.state.tx.us and in the body of such request you must state your email address, full name, mailing address, and telephone number. We will bill you for any fees at that time, if any.

To withdraw your consent with DSHS Contract Management Section

To inform us that you no longer wish to receive future notices and disclosures in electronic format you may:

- i. decline to sign a document from within your signing session, and on the subsequent page, select the check-box indicating you wish to withdraw your consent, or you may;
- ii. send us an email to alison.joffrion@hhsc.state.tx.us and in the body of such request you must state your email, full name, mailing address, and telephone number. We do not need any other information from you to withdraw consent.. The consequences of your withdrawing consent for online documents will be that transactions may take a longer time to process..

Required hardware and software

The minimum system requirements for using the DocuSign system may change over time. The current system requirements are found here: <https://support.docusign.com/guides/signer-guide-signing-system-requirements>.

Acknowledging your access and consent to receive and sign documents electronically

To confirm to us that you can access this information electronically, which will be similar to other electronic notices and disclosures that we will provide to you, please confirm that you have read this ERSD, and (i) that you are able to print on paper or electronically save this ERSD for your future reference and access; or (ii) that you are able to email this ERSD to an email address where you will be able to print on paper or save it for your future reference and access. Further, if you consent to receiving notices and disclosures exclusively in electronic format as described herein, then select the check-box next to ‘I agree to use electronic records and signatures’ before clicking ‘CONTINUE’ within the DocuSign system.

By selecting the check-box next to ‘I agree to use electronic records and signatures’, you confirm that:

- You can access and read this Electronic Record and Signature Disclosure; and
- You can print on paper this Electronic Record and Signature Disclosure, or save or send this Electronic Record and Disclosure to a location where you can print it, for future reference and access; and
- Until or unless you notify DSHS Contract Management Section as described above, you consent to receive exclusively through electronic means all notices, disclosures, authorizations, acknowledgements, and other documents that are required to be provided or made available to you by DSHS Contract Management Section during the course of your relationship with DSHS Contract Management Section.